

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I		
H 0 4 M 3/00		9370-5G	H 0 4 M 3/00	A	
3/42		9667-5G	3/42	A	

審査請求 未請求 予備審査請求 有 (全 82 頁)

(21) 出願番号 特願平8-502274
 (86) (22) 出願日 平成7年(1995) 6月5日
 (85) 翻訳文提出日 平成8年(1996) 12月6日
 (86) 国際出願番号 P C T / U S 9 5 / 0 7 0 7 7
 (87) 国際公開番号 W O 9 5 / 3 5 6 3 3
 (87) 国際公開日 平成7年(1995) 12月28日
 (31) 優先権主張番号 0 8 / 2 5 4 , 5 9 0
 (32) 優先日 1994年6月6日
 (33) 優先権主張国 米国 (U S)

(71) 出願人 ベルサウス コーポレイション
 アメリカ合衆国, ジョージア 30367, ア
 トランタ, ノースイースト, ビーチトゥリ
 ー ストリート 1155番地
 (72) 発明者 ウェイサー, フランク, ジェイ., ジュニ
 ア
 アメリカ合衆国, ジョージア 30328, ア
 トランタ, ハンターズ トレース サーク
 ル 6780番地
 (74) 代理人 弁理士 遠山 勉 (外3名)

最終頁に続く

(54) 【発明の名称】 高度インテリジェントネットワークにおける呼量の取り次ぎ

(57) 【要約】

市内交換会社が動作する高度インテリジェントネットワークと市内交換会社でないサービス・プロバイダーの間のインターフェースを通るデータパケットの呼量の取り次ぎの方法が開示される。このインターフェースは、サービス・プロバイダーと高度インテリジェントネットワークの間に、特に、サービス中継点 (S T P) 等の市内交換会社の装置に接続された S S 7 プロトコルのデータリンクを通して高度インテリジェントネットワークへのアクセスを有するサービス制御点 (S C P) 等のサービス・プロバイダーのネットワーク装置の間に規定される。S T P におけるゲートウェイ・スクリーニングを用いて、市内交換会社でないネットワーク要素から発信されるデータパケットに関してある取り次ぎ手順が行われる。無効な値のデータパケットは拒絶されるが、妥当な値のデータパケットは通されて取り次ぎアクセス S C P へのさらなる取り次ぎ手順に進む。データパケットの何らかのさらなる経路選択 (データパケットの拒絶以外) の前に、取り次ぎアクセス S C P は、データパケットのトランザクション番号等のデータパケットの発信源に関

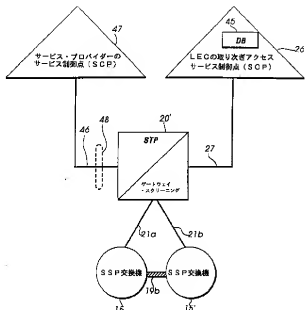


FIG 2

【特許請求の範囲】

1. サービス・プロバイダーのサービス制御点と、少なくとも1つの信号中継点と前記信号中継点に接続されている少なくとも1つの取り次ぎアクセスサービス制御点を含む複数のインテリジェント交換ネットワーク要素、の間での複数のデジタルデータ通信チャネルを含むインテリジェントな交換電話ネットワークの間で承認されないデータパケットメッセージの送信を防止する方法において、

前記信号中継点内でメッセージを受け取る手順、

前記メッセージを前記信号中継点から前記取り次ぎアクセスサービス制御点へと送信する手順、および

前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ手順を含む方法。

2. 前記取り次ぎアクセスサービス制御点が顧客の記録を含む少なくとも1つのデータベースを含み、前記メッセージが第1のトランザクション番号を含み、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記データベース内に前記メッセージのトランザクション識別子を記憶すること、

前記メッセージの第2のトランザクション番号を生成すること、

前記第2のトランザクション番号を前記データベース内の前記第1のトランザクション識別子と関連づけること、

前記第1のトランザクション番号を前記メッセージから取り去ること、および

前記第2のトランザクション番号を前記メッセージに付け加えること

を含む、請求の範囲第1項記載の方法。

3. 前記トランザクション識別子を記憶する前に、前記メッセージをメッセージ情報として読み取る手順、

前記メッセージ情報を、前記データベース内の少なくとも1つの顧客の記録に対応するか比較する手順、および

前記メッセージ情報が前記顧客の記録と対応しない場合には、前記メッセージを拒絶する手順

をさらに含む、請求の範囲第2項記載の方法。

4. 前記トランザクション識別子が、前記第1のトランザクション番号、前記メッセージの発信点コード、および前記メッセージのサブシステム番号を含み、前記トランザクション識別子を記憶する前記手順が、前記第1のトランザクション番号、前記発信点コード、および前記サブシステム番号を記憶することを含む、請求の範囲第2項記載の方法。

5. 前記メッセージが、前記第1のトランザクション番号、前記発信点コード、および前記サブシステム番号を含み、前記第1のトランザクション番号を取り去る前記手順が、前記第1のトランザクション番号、前記発信点コード、および前記サブシステム番号を前記メッセージから取り去ることを含む、請求の範囲第4項記載の方法。

6. 前記第2のトランザクション番号を前記データベース内の活動状態の第2のトランザクション番号のリスト内に記憶する手順をさらに含む、請求の範囲第3項記載の方法。

7. 前記第2のトランザクション番号が割り当てられていない疑似乱数であり、前記第2のトランザクション番号を生成する前記手順が、前記割り当てられていない疑似乱数を前記第2のトランザクション番号として生成することを含む、請求の範囲第3項記載の方法。

8. 前記取り次ぎアクセスサービス制御点が顧客の記録を含む少なくとも1つのデータベースを含み、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記メッセージが応答メッセージであるかどうかを決定すること、

前記メッセージが応答メッセージである場合には、前記応答メッセージのトランザクション番号を前記データベース内の活動状態のトランザクション番号のリストに対応するか比較すること、および

前記トランザクション番号が活動状態のトランザクション番号の前記リスト内の入力と対応しない場合には、前記メッセージを拒絶することを含む、請求の範囲第1項記載の方法。

9. 前記トランザクション番号が活動状態のトランザクション番号の前記リスト内の入力と対応する場合には、前記入力から受信宛先情報を取得する手順、およ

前記受信宛先情報をベースにして前記メッセージの経路を選択する手順をさらに含む、請求の範囲第8項記載の方法。

10. 前記メッセージが、照会メッセージに回答して前記サービス・プロバイダーのサービス制御点から受け取られる応答メッセージであり、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記応答メッセージが発信点コードを含むかどうかを決定すること、

前記応答メッセージが前記発信点コードを含む場合には、前記発信点コードを前記照会メッセージと関連する受信宛先点コードに対応するか比較すること、および

前記発信点コードが前記受信宛先点コードに対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第1項記載の方法。

11. 前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順の後の、前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次がれなかったかどうかを決定する手順、および

前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次がれなかった場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給する手順

をさらに含む、請求の範囲第1項記載の方法。

12. 前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順の後の、前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次ぎにパスしたかどうかを決定する手順、および

前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次ぎにパスした場合には、前記サービス・プロバイダーのサービス制御点がアウトオブサービスであるかどうかを決定する手順、および

前記サービス・プロバイダーのサービス制御点がアウトオブサービスである場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給する手順

をさらに含む、請求の範囲第1項記載の方法。

13. 前記メッセージが特定のサービス・プロバイダーのサービスの要求を含み、前記サービス・プロバイダーのサービス制御点があウトオブサービスであるかどうかを決定する前記手順が前記特定のサービス・プロバイダーのサービスがあウトオブサービスであるかどうかを決定すること、および

前記特定のサービス・プロバイダーのサービスがあウトオブサービスである場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給すること

を含む、請求の範囲第12項記載の方法。

14. 前記信号中継点内でメッセージを受け取る手順の後の、前記メッセージが前記サービス・プロバイダーの信号制御点から発信されているかどうかを決定する手順、および

前記メッセージが前記サービス・プロバイダーの信号制御点から発信されている場合には、最初に前記信号中継点内で前記メッセージを取り次ぐ手順をさらに含む、請求の範囲第1項記載の方法。

15. 前記メッセージが発信点コードを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーのポート識別子を有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が

前記発信点コードが少なくとも1つのポート識別子に対応するか比較すること、および

前記発信点コードが前記ポート識別子のいずれにも対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第14項記載の方法。

16. 前記メッセージが受信宛先コードを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーのメッセージの承認された受信宛先を指定する少なくとも1つの承認されたアドレスを有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が

前記受信宛先コードが少なくとも1つの承認されたアドレスに対応するか比較すること、および

前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第14項記載の方法。

17. 前記承認されたアドレスの1つが前記取り次ぎアクセスサービス制御点のアドレスを含み、前記比較する手順が前記受信宛先コードが前記取り次ぎアクセスサービス制御点の前記アドレスに対応するか比較することを含み、前記拒絶する手順が前記受信宛先コードが前記取り次ぎアクセスサービス制御点の前記アドレスに対応しない場合には前記メッセージを拒絶することを含む、請求の範囲第16項記載の方法。

18. 前記メッセージがサービスインジケータを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーの承認されたサービスを指定する少なくとも1つのサービスインジケータを有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が

前記サービスインジケータが少なくとも1つの承認されたサービスインジケータに対応するか比較すること、および

前記サービスインジケータが前記承認されたサービスインジケータのいずれにも対応しない場合には、前記メッセージを拒絶することを含む、請求の範囲第14項記載の方法。

19. 複数のネットワーク要素の間の複数のデジタルデータ通信チャネルを含むインテリジェント交換電話ネットワークにおけるパケットメッセージの呼量を取り次ぐ方法において、

前記複数のネットワーク要素のうちで新しいTCPメッセージを生成する第1のものにそれぞれの前記新しいTCPメッセージについて第1のトランザクション番号を生成させる手順、

前記複数のネットワーク要素のうちの第2のものに前記TCPメッセージを送信する前記第1のネットワーク要素の前に、前記第1のネットワーク要素に前記第1のトランザクション番号を前記TCPメッセージ内に含ませる手順、

前記第2のネットワーク要素に前記TCPメッセージの単一のトランザクション識別子を作り出させる手順、

前記第2のネットワーク要素に前記TCPメッセージの第2のトランザクション番号を生成させる手順、

前記第2のネットワーク要素に前記TCPメッセージから前記第1のトランザクション番号を削除させる手順、

別の受信宛先に前記TCPメッセージを送信する前記ネットワーク要素の前に、前記第2のネットワーク要素に前記TCPメッセージ内の前記第2のトランザクション番号を含ませる手順、および

前記ネットワーク要素に、前記TCPメッセージと関連する特定のトランザクションに影響を与えるが内部に前記第2のトランザクション番号は含んでいない他のTCPメッセージをその後拒絶させる手順を含む方法。

20. 前記第1のネットワーク要素に、トランザクション識別子のテーブル内に前記第1のトランザクション番号を記憶させる手順をさらに含む、請求の範囲第19項記載の方法。

21. 前記第2のネットワーク要素に、トランザクション識別子のテーブル内に前記単一のトランザクション識別子を記憶させる手順、および

前記第2のネットワーク要素に、前記単一のトランザクション識別子と関連して前記トランザクション識別子のテーブル内に前記第2のトランザクション番号を記憶させる手順をさらに含む、請求の範囲第19項記載の方法。

22. 前記第1のネットワーク要素に前記第1のトランザクション番号を含ませる前記手順が、前記第1のネットワーク要素に前記TCPメッセージ内に前記第1のトランザクション番号およびメッセージ識別子を含ませることを含む、請求の範囲第19項記載の方法。

23. 前記TCPメッセージが発信点コードおよびサブシステム番号を含み、前記第2のネットワーク要素に前記単一のトランザクション識別子を作り出させる前記手順が、前記第1のトランザクション番号を前記発信点コードおよび前記サブシステム番号と連結することによって前記第2のネットワーク要素に前記単一のトランザクション識別子を作り出させることを含む、請求の範囲第23項記

載の方法。

24. 前記第2のネットワーク要素に前記第1のトランザクション番号を削除させる前記手順が、前記第2のネットワーク要素に前記TCA Pメッセージから前記第1のトランザクション番号、前記発信点コード、および前記サブシステム番号を削除させることを含む、請求の範囲第23項記載の方法。

25. サービス・プロバイダーのサービス制御点と、複数のネットワーク要素の間の複数のデジタルデータ通信チャネルを含むインテリジェント交換電話ネットワークの間の、パケットメッセージの呼量を取り次ぐ方法において、

第1のトランザクション番号を有するメッセージを受け取るネットワーク要素に前記メッセージと関連して単一のトランザクション識別子を作り出させる手順、

前記ネットワーク要素に前記メッセージの第2のトランザクション番号を生成させる手順、

前記ネットワーク要素に前記単一のトランザクション識別子に関連して前記第2のトランザクション番号を記憶させる手順、

前記ネットワーク要素に前記メッセージから前記第1のトランザクション番号を削除させる手順、

前記ネットワーク要素に、前記メッセージに前記第2のトランザクション番号を付け加えさせる手順、および

前記サービス・プロバイダーのサービス制御点および前記ネットワーク要素に、その後、前記メッセージと関連する特定のトランザクションに影響を与える他のメッセージ内の前記第2のトランザクション番号を含ませ、前記第2のトランザクション番号を含んでいない前記他のメッセージを拒絶させる手順を含む方法。

26. 前記メッセージが発信点コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーのポート識別子を有し、

前記ネットワーク要素に前記発信点コードが1つのポート識別子に対応するか比較させる手順、

前記発信点コードが前記ポート識別子のいずれにも対応しない場合には、前記

ネットワーク要素に前記メッセージを拒絶させる手順

をさらに含む、請求の範囲第25項記載の方法。

27. 前記メッセージが受信宛先コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーのメッセージの承認された受信宛先を指定する少なくとも1つの承認されたアドレスを有し、

前記ネットワーク要素に前記受信宛先コードが少なくとも1つの承認されたアドレスに対応するか比較させる手順、

前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には、前記ネットワーク要素に前記メッセージを拒絶させる手順をさらに含む、請求の範囲第25項記載の方法。

28. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーの承認されたサービスを指定する少なくとも1つのサービスインジケータを有し、

前記ネットワーク要素に前記サービスインジケータが少なくとも1つの承認されたサービスインジケータに対応するか比較させる手順、

前記サービスインジケータが前記承認されたサービスインジケータに対応しない場合には、前記ネットワーク要素に前記メッセージを拒絶させる手順を含む、請求の範囲第25項記載の方法。

29. サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点の法定の中継回線のグループのインデックスのテーブルを維持させる手順、

前記ある特定のの中継回線のグループの経路選択の要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記取り次ぎアクセスサ

サービス制御点に前記特定の中継回線のグループの経路選択に対応する入力の前記テーブルをチェックさせる手順、および

前記特定の中継回線のグループの経路選択が前記テーブル内の入力に対応しない

場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順

を含む方法。

30. サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点のネットワーク要素の承認された加入者電話番号のテーブルを維持させる手順、

ネットワーク要素へのアクセスの要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記取り次ぎアクセスサービス制御点に前記ネットワーク要素の加入者電話番号に対応する入力の前記テーブルをチェックさせる手順、および

前記加入者電話番号が前記テーブル内の入力に対応しない場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順

を含む方法。

31. サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点の許された資源占有数を維持させる手順、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点が占有している資源の現在のカウン트를維持させる手順、

ネットワーク資源の使用の要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記現在のカウン트가前記許された資源占有数

と等しいかそれよりも大きい場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順を含む方法。

3 2. サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス

制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に、前記サービス・プロバイダーのサービス制御点が予め選択した期間内に戻さないメッセージの現在のカウントを維持させる手順、

前記現在のカウントが予め選択したカウントと等しいかそれよりも大きい場合には、前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点に供給されるメッセージの数を減らさせる手順を含む方法。

3 3. 前記取り次ぎアクセスサービス制御点にメッセージの数を減らさせる前記手順が、前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点に向けられた次のメッセージを拒絶させることを含む、請求の範囲第3 2項記載の方法。

3 4. 前記ネットワークが前記サービス・プロバイダーのサービス制御点をサービスする少なくとも1つのサービス交換点を含み、前記取り次ぎアクセスサービス制御点にメッセージの数を減らさせる前記手順が、前記取り次ぎアクセスサービス制御点に自動発呼ギャッピングのメッセージを前記サービス交換点に送らせることを含む、請求の範囲第3 2項記載の方法。

3 5. 前記アウトオブサービスのサービス・プロバイダーのサービス制御点をテストする手順、

前記アウトオブサービスのサービス・プロバイダーのサービス制御点が前記テストに適切に応答する場合、前記アウトオブサービスのサービス・プロバイダーのサービス制御点を使用可能状態のサービス・プロバイダーのサービス制御点として再分類する手順

をさらに含む、請求の範囲第 1 2 項記載の方法。

3 6. 前記アウトオブサービスのサービス制御点をテストする前記手順が、前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを送ることを含む、請求の範囲第 3 5 項記載の方法。

3 7. 前記アウトオブサービスのサービス制御点をテストする前記手順が、前記

アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを定期的なペースで送ることを含む、請求の範囲第 3 6 項記載の方法。

3 8. アウトオブサービスのサービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを送る手順、

前記アウトオブサービスのサービス・プロバイダーのサービス制御点が前記テストメッセージに適切に応答する場合、前記アウトオブサービスのサービス・プロバイダーのサービス制御点を使用可能状態のサービス・プロバイダーのサービス制御点として再分類する手順

を含む方法。

3 9. 前記アウトオブサービスのサービス制御点にテストメッセージを送る前記手順が、前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを定期的なペースで送ることを含む、請求の範囲第 3 8 項記載の方法。

4 0. サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に、データパケットメッセージ内の前記取り次がれた呼量に関する監査できる事象を認識させる手順、

前記監査できる事象の監査証跡を作り出す手順
を含む方法。

4 1. 前記監査できる事象がメッセージを含み、前記監査証跡が、日付、時間、トリガのタイプ、および前記メッセージのトリガする受信宛先番号および前記メッセージの写し、を含み、前記監査できる事象の監査証跡を作り出す前記手順が、前記日付、前記時間、前記トリガのタイプ、および前記メッセージの前記トリガする受信宛先および前記メッセージの前記写し、を含む前記監査証跡を作り出すことを含む、請求の範囲第40項記載の方法。

4 2. サービス・プロバイダーのサービス制御点と、インテリジェント交換電話ネットワーク内の複数のネットワーク要素の間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記ネットワーク要素のうちの1つ内に、セキュリティ監査要求のパラメータを含むメッセージを受け取る手順、および

前記セキュリティ監査要求のパラメータを受け取ることに応答して、前記ネットワーク要素のうちの前記1つに前記メッセージのセキュリティ・パラメータを作り出させる手順

を含む方法。

4 3. 前記ネットワーク要素に、その後前記メッセージと関連する特定のトランザクションに影響を与える他のメッセージのある(with)前記セキュリティ・パラメータを含ませる手順

をさらに含む、請求の範囲第42項記載の方法。

【発明の詳細な説明】

高度インテリジェントネットワークにおける呼量の取り次ぎ

関連出願の相互参照

この出願は、発明の名称「公衆電話ネットワーク用のオープンな高度インテリジェントネットワークのインターフェースの取り次ぎ」に係る 1993 年 6 月 28 日提出の合衆国特許出願第 083、984 号の一部継続出願であり、且つ、発明の名称「共同命令実行環境によるオープンな高度インテリジェントネットワークのインターフェースの取り次ぎ」に係る 1994 年 5 月 20 日提出の合衆国特許出願（出願人代理人整理番号 19260-0410）の一部継続出願である。本出願人はこの参照により、同時に係属し、且つ、共有された上記特許出願を併合する。

技術分野

本発明は、交換式電話による通信の分野に関し、特に、現代の電話交換システムに関連する高度インテリジェントネットワーク（A I N:Advanced Intelligent Network）へのアクセスを電話サービス・プロバイダー以外の広範囲のエンティティに与えることによって許されるであろうメッセージ内容およびネットワークの影響の取り次ぎの方法である。

背景技術

米国において電話サービスが利用できるようになってからの 1 世紀余りの間に、公衆電話システムの複雑さ、大きさ、および性能は、絶えず発展し発達してきた。発呼を交換し完了する配線盤を操作する人間のオペレータによって発呼の経路が選択されてきた時代から、システムの容量は、呼量においてもサービスのオプションの量においても非常に増してきた。電話会社の電話局または電話局交換機は、それぞれが顧客の電話装置を終端とする多数の加入者回線が接続される装置である。従来の住居用の電話サービスについては、加入者回線には 1 個またはそれ以上の電話機が接続される。さらに電話局は、その電話局を他の電話局に接続する

多数の中継回線を有する。事務所に構内交換機（P B X: private branch excha

nge) の交換機を供給する中継回線等の他の中継回線も、顧客に提供されている。

改善された電話サービスの初期の発展のひとつは、1960年代初期における加入者長距離市外ダイヤル方式の導入である。それ以前は、長距離市外通話はすべて、1人またはそれ以上の人間のオペレータが取り扱わねばならず、オペレータが呼線を設定しビリング装置を起動していた。加入者長距離市外ダイヤル方式を可能にした技術の重要な特徴のひとつは、ダイヤルされたディジットすなわち被呼番号を識別するデータを集め、記憶し、転送する交換機の性能である。これらは、発呼が多周波(MF: multifrequency)信号としてよく知られている信号体系を経由して設定されるときに、ネットワークを通して伝送された。MF信号は、情報信号(被呼番号を識別するもの)が、いったん発呼が完了すると音声信号を搬送する中継回線と同じ中継回線を介して、音声周波数帯域内の信号によって伝送された、という点において、帯域内周波信号方式の1種である。この技術によって、取り扱われる長距離の呼量がずっと多くなり、1960年代および1970年代の米国において電話サービスをかなり改良しより多くのサービスを求める要求を満たす助けとなった。帯域内周波信号方式技術の主な欠点は、発呼の設定の間、音声の中継容量(voice trunk capacity)が占有される、ということであった。さらに、相手側の発呼番号が話し中である等何らかの理由によって発呼を完了することができない場合、発呼の設定がネットワークを通るその道筋を切り替えて話し中の報告が音声回線を介して発呼者に戻される間、長距離の中継容量が占有されてしまった。5分から10分でも、1日に何千もの話し中の通話があると、中継容量をかなり使用することになる。

1970年代の後期および1980年代の初期において、米国電話電信会社(AT&T: American Telephone & Telegraph Company)は初期の種類のオフィス間共通線信号方式(CCIS: common channel interoffice signaling)を開発した。CCISは、本質的に、電話の発呼についての情報が、発呼自体の信号の伝送に用いられる音声回線とは別個の高速データリンクを介して伝送される、交換電話ネットワークのネットワーク・アーキテクチャである。オフィス間共通線信号方式の開発の初期においては、音声リンクを設定する中継回線容量を割り

当てる前に発呼を完了できるかどうかを最初に決定することができる高速デジタルデータを提供するように、オフィス間データ信号リンクを設計することができると認識されていた。従って、オフィス間共通線信号方式では、アトランタにいる発呼者がシアトルの番号をダイヤルする場合には、被呼番号の識別を、アトランタにある発呼側の電話局からシアトルにある被呼側の電話局にオフィス間信号データリンクを介して伝送することができる。被呼側の電話局は、被呼番号にサービスを提供する電話局である。被呼番号が話し中の場合には、この情報を提供するデータがオフィス間信号リンクを介してアトランタにある発呼側の電話局に伝送で戻され、このアトランタにある電話局が、市内で話し中音を発呼者に提供する。従って、この処理の間に長距離中継回線容量が占有されることはなく、以前の方式であれば発呼を完了しようとして用いられたであろうアトランタとシアトルの間の音声回線は、他の使用への余地を残している。シアトルの被呼番号が話し中でない場合には、ネットワーク内の様々な装置がこの発呼に関する情報に応答し、その発呼の接続を設定するオフィス間中継回線が割り当てられ、発呼が完了する。

公衆電話ネットワークは、１９８０年代に、複合的で非常に用途が多いシステムに発展した。その大部分は、オフィス間共通線信号方式の１形式をサポートし、それによって制御されている。このネットワークの基礎は、ＡＴ＆Ｔが設計した。司法的な命令により１９８４年にＡＴ＆Ｔが市内交換会社（ＬＥＣ：local exchange carriers）を分割してからは、ベル地域経営会社（ＲＢＯＣ：Regional Bell Operating Companies）その他独立した市内電話サービス・プロバイダーがこのネットワークの開発を継続している。交換電話ネットワークの基本アーキテクチャは、かなりの部分において、米国、および西ヨーロッパや日本を含む先進工業化世界全体にわたって、同一である。本明細書で説明する現在のネットワークの詳細は、ＲＢＯＣその他米国内で操業している市内交換会社が用いているものである。このネットワーク・アーキテクチャは、米国における現代の電話交換システムのすべてが用いており、西ヨーロッパおよび日本における現代のシステムと略同一である。

現代のオフィス間信号は、信号方式７（ＳＳ７：signaling system 7）と呼

れるプロトコルを用いてデジタルリンクを介して起こる。SS7については、以下により詳細に触れる。高度インテリジェントネットワーク（AIN:Advanced Intelligent Network）は、以下の特性を有しているという点において、現在のオフィス間信号の拡張集合とみなしてもよい。第一に、これもSS7プロトコルを用いている。基本的に、高度インテリジェントネットワークは、トリガとして知られているAINメッセージを生成し適切な応答を行う資源および相互接続を集めたものである。トリガとは、新しいAINメッセージ・シーケンスを生成するある特定の事象である。市内交換会社の顧客は、ある特定のトリガの事象に関してAINに提供されるトリガを有することに対して料金を支払わねばならない。例えば、ある番号への着信に関する特殊なサービスを受けるためには、その加入者電話番号の顧客は通常、成端試みトリガ(termination attempt trigger)を契約せねばならない。これによって、誰か加入者がその特定の加入者電話番号に通話を申し込もうとしたことをネットワークが検出するときにはいつでも、AINメッセージが生成される。すると、サービス制御点がデータベースに情報を求め、トリガが受け取られたことを考えればその発呼の取り扱いについてどのような非標準の応答が適切であるかを決定する。米国において電話事業に精通した人々の多くが近い将来に起こると考えている次のような出来事の結果として、本発明が必要となる。すなわち、市内交換会社が動作する高度インテリジェントネットワークへのアクセスが第三者に提供され、第三者が市内交換会社の加入者に対して競合する電話関連サービスを提供することができる、という出来事である。言い換えれば、任意にせよ規制的な命令によってにせよ、市内交換会社（LEC: local exchange carriers）（すなわち、市内電話サービス・プロバイダー）は、音声接続の設定および切断を含む、電話会社が提供する現代の特徴およびサービスを支配する高度インテリジェントネットワークへのアクセスを、他者に許さなければならなくなることが予想される。

現代のインテリジェント公衆電話ネットワークにおいても、基本的な発呼の設定、切断、および経路選択に用いる上記の信号パスと同じ信号パスが用いられて

、強化したカスタム発呼の特徴を提供し、ビリング装置の動作を制御して課金記録を保っている。従って、このネットワークに市内交換会社以外のものがアクセス

することを許すということは、危険を伴う計画である、ということが理解されよう。電話システムを制御するデジタルネットワークにアクセスしそのネットワーク内に記憶された情報にアクセスする者が不注意または悪意であれば、第三者へのアクセスが行われるときに適切な予防措置を講じない限り、公衆電話ネットワークの正しい動作がひどく妨げられたり、課金データを含むネットワーク内に記憶された情報が改ざんされたり、ネットワーク内に記憶された個人情報不正に入手されたりする可能性がある。従って、本発明は、公衆電話システムのインテリジェントネットワークへのアクセスがオープンになることを見越してなされた。

本発明の必要性および本発明の実施の両方を理解するためには、まず最初に、現代の高度インテリジェントネットワークの基本アーキテクチャおよびインターフェースが第三者に提供される可能性があるという点を理解することが必要である。本明細書の図1は、典型的な市内交換会社のA I Nの少なくとも一部を示すブロック図である。このブロック図は簡単であるが、その構成要素は当業者にはよく知られている。典型的な公衆電話ネットワーク内には、複数の電話局交換機が設けられている。サービス交換点（S S P: Service Switching Point）が、現代の電話局交換機のA I N構成要素である。これを、図1にS S P交換機15-15'として示す。15と15'の間の破線は、数が任意であることを示している。また、交換機16等のS S Pでない交換機も、ネットワークに含まれている。

S S P電話局交換機とS S Pでない電話局交換機の違いは、前者がインテリジェントネットワークの機能性を含んでいるということである。これは、その交換機が適当なハードウェアおよびソフトウェアを装備していて、1組の所定の状態が検出されると、交換機が加入者回線上の所定の発呼状態のトリガを開始し、A I Nを介して送られるべき適切なメッセージとしてそのトリガを生成し、ネット

ワークからある行動をとるように命令する応答を受け取るまでは発呼の取扱を保留するようになっている、ということを示す。または、交換機は、タイムアウトが起こって交換機が行った照会に対してネットワークが何の返答もしない場合に実行する省略時タスクを有する。要するに、SSP交換機とは、本明細書において説明する高度インテリジェントネットワークを扱い利用するように十分装備されたものである。

SSPでない交換機16は、電子スイッチであって、ある基本パケット (rudimentary packets) を生成してネットワークを介して提供することができるが、かかる交換機に接続された加入者回線にインテリジェントネットワークで利用できるより複合的な特徴およびサービスを提供するためには、以下により詳細に説明する他の装置に依存せねばならない。電話局15-15'、16はそれぞれ、一般に17-17'で示す、接続された複数の加入者回線を有する。通常、加入者回線の数、10,000から70,000回線程度である。加入者回線17-17'のそれぞれは、顧客の構内装置の終端部分に接続されている。この終端部分は、交換機のそれぞれについての同様の複数の電話機18-18'で示す。

電話局交換機15、16を接続しているのは、図1に19a、19bで示す複数の中継回線である。これらは、電話局を相互接続する音声パス中継回線であり、発呼が完了したときにはこれらを介して接続される。通常の都市の環境における電話局の中継回線は、図1が暗示するようなヒナギクの花をつなげた輪のような配列に制限されるものではない、ということが理解されるべきである。言い換えれば、通常のネットワークにおいて、中継回線は電話局交換機15'と電話局交換機16の間に存在する。従って、2つの電話局の間で市内発呼が行われる場合には、これらの電話局を直接中継する接続が存在ししかもその中継回線が話し中でない場合には、ネットワークはその中継回線をその特定の発呼の完了に割り当てる。この2つの電話局を直接中継する回線がなかったり、回線はあるがすべて話し中である場合には、発呼は発呼側の電話局から少なくとも1個の他の電話局への中継回線に沿い、それに続く中継回線の接続を通して被呼側の電話局へと経路が選択される。

この一般的なアーキテクチャは、多数の市内交換会社を含むより広範囲の地理的地域を考える場合に、拡大される。その場合には、重要な違いは、長距離中継回線のみを交換する相互交換会社の交換機(inter exchange carrier switches)が含まれている、ということだけである。

インテリジェント交換電話ネットワークのインテリジェンスの大部分は、図1に示す残りの構成要素にある。これらは、上述のオフィス間共通線信号体系の現在のバージョンを実施するコンピュータおよび交換機である。交換機15ないし

16のそれぞれは、それぞれデータリンク21a、21b、および21cを介して、市内(localの)信号中継点(STP: signal transfer point)20に接続されている。現在これらのデータリンクは、信号方式7(SS7: Signaling System 7)と呼ばれる信号プロトコルを用いる、56キロビット/秒の双方向性データリンクである。SS7というプロトコルは、当業者にはよく知られており、米国国家規格協会(ANSI: the American National Standards Institute)が公表している仕様書に説明されている。SS7というプロトコルは、層状プロトコルであり、それぞれの層がその上の各層にサービスを提供し、それぞれの層にサービスを提供するのにその下の各層に依存している。SS7プロトコルはデータパケットを用いる。データパケットは、パケット、情報パケット、メッセージパケット、またはメッセージと呼ばれることもあるが、どれも同じものを指す。データパケットは、通常の初めおよび終わりフラグおよびチェックビットを含む。さらに、可変長のユーザ固有のデータおよび経路選択ラベルを含む、信号情報フィールドが設けられている。メッセージの優先順位、メッセージの受信宛先の国内ネットワーク、およびメッセージを作り出したエンティティを識別するユーザ名、を識別するサービス情報オクテットが設けられている。また、パケット内には制御およびシーケンス番号も含まれており、その使用および受信宛先は当業者にはよく知られており、上に参照したANSI仕様書内に説明されている。

SS7プロトコルの主な特徴のひとつは、その層状の機能構成である。SS7プロトコルの転送機能は、4つのレベルに分けられる。そのうちの3つは、メッ

セージ中継部（MTP：Message Transfer Part）を構成する。4つ目のレベルは、共通の（common）信号接続制御部（SCCP：Signaling Connection Control Part）からなる。SS7プロトコルは、以下の4つの基本的なサブプロトコルからなる。メッセージ中継部（MTP）、これは、信号点（Signaling points）間の信号メッセージの基本的な経路選択の機能を提供する。信号接続制御部（SCCP）、これは、信号点間の発呼の設定以外のメッセージの中継のためのさらなる経路選択および管理機能を提供する。統合ディジタル通信サービスユーザ部（ISUP：Integrated Services Digital Network）、これは、信号点間の発呼の設定の信号情報の中継に備える。そして、トランザクション性能アプリケーション部（T

CAP：Transaction Capabilities Application Part）、これは、信号点間の回線に関係しない情報の中継に備える。

交換機からのSS7データパケットは、すべて信号中継点（STP）20に行く。当業者であれば、信号中継点20は単に、SS7プロトコルの適切な層内の経路選択情報に回答しパケットをその意図する受信宛先に送るようにプログラムされている単なる多ポート高速パケット交換機である、ということがわかるであろう。信号中継点は、通常、それ自体パケットの受信宛先ではなく、単に、データパケットを生成しデータパケットに回答するネットワーク上の他のエンティティの間の呼量を管理する。STP20等の信号中継点装置が従来ネットワーク内に冗長なペアを組んで設備されており、1個の装置が故障しても、最初のSTPがサービスに戻ることができるまでそれとペアになっているもう一方が引き継ぐようになっていることに注意するべきである。実際は、信頼性をさらに高めるために、電話局交換機15ないし16のそれぞれの間に冗長データリンクがある。図面を簡単にするために、冗長装置は本明細書の図面には示していない。

信号中継点20には、SS7データリンク25を介して、1AESSのネットワークアクセスポイント（NAP：network access point）22も接続されている。ネットワークアクセスポイント22は、トリガの状態を検出するようにプログラムされた計算装置であり、AINのネットワークシステムにこれらのトリガ

が検出されたことを告知するのに、SSP交換機をサポートを必要とする。1個のSSPで多数のNAP交換機をサポートすることができる。論理的に、このSSPは、もしSSPを装備した交換機であったならば1AESSのNAPに送られるネットワークが生成するパケットの多くの、受信宛先として指定されている。

情報の大半、およびネットワークの新しい強化した特徴の多くの基礎は、SS7データリンク27を介して信号中継点20に接続された市内サービス制御点（SCP：service control point）26にある。当業者には知られているように、サービス制御点は、比較的パワフルな故障を許容するコンピュータによって、物理的に実施される。典型的な実施装置は、どちらも米国電話電信会社販売の、スターサーバー（Star Server）FTモデル3200、またはスターサーバーFTモデル3300を含む。これらのコンピュータのアーキテクチャは、それぞれタンド

ム社のインテグリティ（Integrity）S2およびインテグリティS1のプラットフォームをベースにしている。公衆電話ネットワークの大部分の実施においては、信頼性およびネットワークが続いて動作することを確実にするために、サービス制御点も冗長に接続したペアを組んで設けられている。

サービス制御点を実施する計算装置は、通常、1個のドライブにつき300メガバイトから1.2ギガバイトの範囲のディスクドライブを1個から27個収容でき、24から192メガバイト程度のメインメモリを有する。従って、これらが大型でパワフルな計算マシンであるということが理解されよう。サービス制御点が果たす各機能の中に、強化したサービスを提供するのに用いるネットワークのデータベースの維持がある。SCPを実施するコンピュータは、1秒あたり1700万個程度の速度で命令を実行することができる。SS7プロトコルを用いると、これは1秒あたり約50から100個のネットワークのメッセージのトランザクション（照会／応答のペア）になる。

サービス制御点のコンピュータは最初、800番サービス、すなわちフリーダイヤル（発呼者にとって）の長距離サービスの実施に必要なトランザクションお

および課金トランザクションを取り扱うためにネットワークに導入された。800番の加入者は、その加入者の800番の番号に通話が申し込まれると発呼される少なくとも1個のダイヤル呼び出し方式の回線の番号を有している。この800番の市外局番に対応する物理的な電話局や国の地域はない。多くの電話局交換機でその度に変換情報を提供するよりも、800番通話の加入者電話番号の索引を作ることができる中心位置(central locations)をいくつか設ける方がかなり経済的である。現在、サービス制御点は、クレジットカード通話のトランザクションのデータベースも含む。

また、サービス制御点は、ある特定のサービスの顧客を識別するデータベースも含む。交換機15-15'等の交換機におけるデータおよび発呼の処理をできる限り簡単で一般的なものにしておくために、それぞれの発呼について交換機において比較的小さな組のトリガが規定されている。このネットワークにおけるトリガは、サービス制御点に送られるパケットを生成するある特定の加入者回線と関連する現象である。このトリガによって、サービス制御点はそのデータベース

に照会を行い、この特定の発呼について何らかのカスタム化した発呼の特徴または強化したサービスを実施するべきか、あるいはその発呼に従来の普通のダイヤル呼び出し方式の電話サービスを提供するべきかを決定する。データベースの照会の結果は、SCP26からSTP20を通過して交換機に送り戻される。

戻りパケットは、その発呼の処理方法に関する交換機への命令を含む。この命令は、カスタム化した発呼サービスまたは強化した特徴の結果として何か特別な行動を取ることもよいし、あるいは単に、その特定の発呼に何か普通の電話サービス以外のものを提供するべきだということを示す入力があるデータベースにないということを示すものでもよい。後者のタイプのメッセージを受け取る場合、これに応答して、交換機はその発呼状態を通過し、被呼ディジットを集め、その発呼を設定しその経路を選択するのに用いられるさらなるパケットを生成する。これについては上に説明したとおりである。

様々な市内交換会社の中で発呼の経路を選択する同様の装置が、地域信号中継点28および地域サービス制御点29において設けられている。地域STP28

は、SS7データリンク30を経由して市内STP20に接続されている。地域STP28は、対応する市内装置間のデータリンク27と物理的にも機能的にも同じデータリンク31を経由して、地域SCP29と接続されている。市内装置と同様、信頼性を高くするために、地域STPおよびSTCは冗長に接続したペアを組んで設けられている。

市内および地域のサービス制御点26、29の両方が、それぞれのデータリンク35、36を経由して、サービス管理システム（SMS：service management system）37に接続されている。このサービス管理システムもまた、大型の汎用デジタルコンピュータおよび市内交換会社および相互交換会社の事務所へのインターフェースによって実施されている。サービス管理システムは、加入者がそのAINサービスを全体的に変更する場合にサービス制御点26、29のデータベースに情報をダウンロードする。同様に、サービス管理システムは、リアルタイムでないペースで、電話会社の加入者に提供したサービスのインボイスを適切に作るために必要な課金情報をダウンロードする。

現代の高度インテリジェントネットワークはまた、図1に示すサービス接続点

39等のサービス接続点（SN：service node）も含む。当業者であれば、サービス接続点には精通しており、サービス接続点は物理的にはサービス制御点26、29を実施するのと同じタイプのコンピュータによって実施される。サービス接続点39は、計算性能がありデータベースを維持するという特徴に加え、音声およびDTMF信号認識装置、および音声合成装置も含む。サービス接続点39は、データリンク40を経由して、SCP26、29にサービスを提供するのと同様の方法でサービス接続点にサービスを提供するサービス管理システム37に接続されている。サービス接続点39は、物理的にはSCP26と非常に似ているが、その使用においては、重要な違いがいくつかある。SCP26等サービス制御点は通常、発呼を送ったり800番の変換や経路選択等の大量経路選択サービスを実施する。また、クレジットカード番号のバリデーション等の課金の承認のための大量データベースを維持しそれへのアクセスを提供するのにも用いられている。市内交換会社ネットワークの大部分において、サービス制御点は、発呼

の論理的完了、すなわち被呼加入者回線への呼び出し信号の供給および発呼加入者への呼び出しに先だって行われるデータベース検索および経路選択サービスにのみ用いられる。

これとは対照的に、サービス接続点 3 9 等のサービス接続点は主に、発呼への音声接続、あるいは発呼の間またはその後に交換された接続を経由して加入者にかなりの量のデータの転送を必要とする何らかの強化した特徴またはサービスが必要な場合に用いられる。図 1 に示すように、サービス接続点 3 9 は通常、4 1 で示す統合デジタル通信サービス (ISDN: Integrated Service Digital Network) リンクを経由して 1 個またはそれ以上の (しかし通常数個のみの) 交換機に接続されている。したがって、発呼中に (すなわち、呼び出し信号の完了または被呼加入者のピックアップの後) 実施されるサービスは通常、サービス接続点 3 9 等のサービス接続点の設備を用いる。

読み手のために例を挙げると、発呼者の音声による告知は、サービス接続点 3 9 を経由して実施されるカスタムの特徴である。ある加入者が別の加入者であるジョーンズさんの番号をダイヤルし、ジョーンズさんは入呼びの音声による告知を提供するサービスを契約していると仮定しよう。SSP を装備した交換機の発

呼進行状態のうちのひとつが、ダイヤルされたディジットを集めた後、交換機が成端要求トリガを生成するときに起こる。このトリガは、STP 20 を通って SCP 26 へと経路選択されその特定の被呼者番号を識別する SS7 データパケットからなる。SCP は、記録を検索してジョーンズさんの電話回線と関連する加入者電話番号を探し、彼女が、入呼びを識別する音声による告知を提供するサービスの加入者であることを検出する。すると SCP 26 は、パケットをデータリンク 27 を介して STP 20 に送り返し、パケットは発呼者の加入者回線と関連する電話局とジョーンズさんの加入者回線と関連する電話局の両方に送られる。

発呼者の電話局は、待機するかまたは発呼者の加入者回線に再度、折り返し呼び出しを行うように指示される。別のパケットが、交換機 15' に送られる。このパケットには、ジョーンズさんの加入者電話番号、発呼者の番号、およびサービス接続点 3 7 における音声合成機のチャンネルへのアクセスの要求、を含む。交

交換機 15' は、ISDN リンク 41 を経由してサービス接続点と音声およびデータ回線を接続し、パケット（適切な ISDN のフォーマットの）をサービス接続点に通す。するとサービス接続点は、そのデータベースに照会を行って、ジョーンズさんの記録（実際には彼女の加入者電話番号の記録）にその特定の発呼番号の入力があるかどうかを決定する。

一方で、電話局 15' とジョーンズさんの電話回線を担当する電話局の間で、必要な音声継回線が接続されており、従って、ジョーンズさんの加入者回線に応答監視信号が戻されるときには、サービス接続点 39 における合成機とジョーンズさんの間には音声パスが存在している。すると合成機は、発呼者の識別を告知し、ジョーンズさんの電話に出ている人は、適切な行動（電話上のある特定の番号を押す、等）をとって、その電話に出たいかどうかを示すことができる。DTMF 番号は、サービス接続点における DTMF 認識回線によって認識され、これも同様に、音声回線に繋がれる。するとサービス接続点は、その発呼が受諾されたか拒絶されたかを示す適切なパケットを生成し、それらのパケットは ISDN リンク 41 を経由して交換機 15' に進む。交換機において、プロトコルの変換が行われ、これらのパケット内の情報が適切な SS7 プロトコルのパケットにフォーマットされ、そして信号中継点 20 に通され、適切な局に送られて、発

呼者とジョーンズさんの加入者回線間の音声リンクを設定するか、または適当な音響式確認（話中音やリオーダー音等）を発呼者に提供する。

前述の説明は、現在の公衆電話システムである高度インテリジェントネットワークの動作を、いくつか例を挙げて基本的に概観するものである。当業者にも、偶然本明細書を読んで興味を持った人にも明らかとなるとおり、ネットワークを通るデータパケットのインテグリティ（完全さ）は、ネットワークの動作にとってきわめて重大である。システムが正しく機能して発呼が完了するように、パケットのインテグリティは維持されねばならない。また、SS7 データパケットが音声回線容量の割り当てを制御するので、ネットワークが正しく動作するためには、中継回線容量に対するスプリアス（偽の）の、つまり不要の要求がネットワーク内で生成されないことが決定的に重要である。

本発明の発明者は、ネットワークのSS7データリンクを第三者にオープンにして、第三者が電話ネットワークを介してカスタム化したサービスを提供できるようにすることが、第三者のプロバイダーが提供するサービスの性質について市内交換会社に広範な情報を提供する必要がなくなるように規定される、と考えている。従って、ネットワークを、第三者である強化した発呼サービスの供給者にオープンにする見込みであるということは、市内交換会社のネットワークと第三者の間のインターフェースにおいて注意して取り次がねばならず、アクティビティおよびデータパケットのメッセージを監視してネットワークのインテグリティおよび動作、およびサービス・プロバイダーの加入者すべてのプライバシー、の両方を保護せねばならない、ということである。

また、ネットワーク内のデータベースに維持されている情報の多くは、市内交換会社（LEC）の顧客の機密に関わる商業上の情報を構成する可能性がある。企業が電話を受ける度合い、企業が受ける800番の呼量、あるいは特定の企業への電話の時間的特性さえも、LECの顧客のライバルにとって有用かもしれない情報を構成する可能性がある。従って、ネットワークがオープンになる場合には、注意深くチェックしてLECの顧客以外の者がアクセスできる情報のタイプを制限する必要がある。

発呼の経路選択を制御する別個のSS7の信号パケットを現在使用するように

なったのは、かなりの部分、カスタム発呼サービスまたは強化したサービスを提供するために発呼の経路を変更する必要があったからである。この最も簡単な例は、もちろん、1本の加入者回線向けに意図された発呼を別の1本に転送する、ということである。しかし、発呼の経路を変更してダイヤルされた番号と関連するもの以外の加入者回線に送ることができるということはまた、ネットワークが第三者であるデータパケットのジェネレータにオープンになったときには、潜在的な商業上の悪影響にも通じるものである。

例えば、重要な新顧客源として入電話を用いている企業のライバルは、野放しにされていれば、サービス制御点のコンピュータに、そのネットワークのメッセージを生成した企業の電話にライバルから電話を転送するように命令するパケッ

トをネットワーク上に生成することができる。これを定期的に行って、転送命令を短期間だけ適当な位置になるようにし、ある割合の入呼びをこのような方法で抜き取ることができる。従って、ネットワークが第三者にオープンになる場合には、承認されていないまたは不適切な、発呼の経路変更や発呼への干渉を行おうとする試みから、発呼の経路選択の処理のインテグリティを保護し、ネットワークにアクセスできる第三者の存在が影響を与えないようにすることが必要である。

要約すると、高度インテリジェントネットワークは、電話の通話の取り扱いに多くの用途を開く、複合的高速高呼量バケット交換のメッセージを送る方法である。大部分のネットワーク要素は、そして特にSSP交換機は、ある事象があると比較的簡単なフォーマットの照会メッセージが生成され、発呼の処理を続行する前にネットワークからの応答を待つように設計されている。これらの手順には、照会に対する応答が受け取られない場合にはタイムアウトするウォッチドッグタイマが用いられる。しかし、さらなる発呼の進行が、有効な応答と対比されるタイムアウトが起きることにより制御される状況では、処理している発呼のうちかなりの割合について、ネットワークの性能がかなり劣化する。そうすると、顧客は発呼処理で過度に遅れたり、強化した特徴の提供を適切に受けることができない、ということを経験することになる。本質的に、ネットワークを多用途に使えるようにすると、そのネットワークは不適切なネットワークのメッセージに対して脆弱になる。従って、ネットワークをオープンにして、第三者である強化し

たサービス・プロバイダーに高度インテリジェントネットワークへのアクセスができるようにすると、市内交換会社と第三者であるサービス・プロバイダーの間のインターフェースを通るメッセージの呼量の取り次ぎを行い、第三者であるサービス・プロバイダー側のインターフェースでの悪影響、人的エラー、および装置の故障からネットワークを保護する必要がある。

発明の概要

本発明は、SS7プロトコルのオープンなアクセス環境においてネットワーク

要素の使用によりオープンな高度インテリジェントネットワーク環境における高度インテリジェントネットワークのメッセージの呼量を取り次ぐ方法である。より詳細には、本発明の好適な形態は、多数のサービス・プロバイダーのサービスに関する命令を供給するサービス・プロバイダーのSCPから受け取られたまたはそこへ向かうデータパケットに関して、STPにおいておよび取り次ぎアクセス(mediated access)SCPにおいて取り次ぎ手順を用いることによって、高度インテリジェントネットワークにおいて達成される。

高度インテリジェントネットワークを、市内交換会社でないサービス・プロバイダーにオープンにすることによって、一方で、システム内のすべての要素に、高度インテリジェントネットワークのメッセージの受信宛先および応答の適切な受信宛先を明白に検出させる必要性和、他方で、サービス・プロバイダーが高度インテリジェントネットワークへのアクセスを悪用してライバルに関する情報に不適切なアクセスをしたり、どうにかしてネットワークの動作やシステム上のある特定のライバルのアプリケーションの動作を妨害する、ということができないように保証する必要性との間に、緊張関係が作り出される。

高度インテリジェントネットワークへの承認されていないアクセスを防止するために、本発明は、STPにおけるゲートウェイ・スクリーニングを用いて、サービス・プロバイダーのSCP等の市内交換会社のものではないネットワーク要素から発信されたデータパケットに関してある取り次ぎ手順を行う。STPは、データパケットに、妥当な発信コード、妥当な受信宛先コード、妥当なサービスインジケータがあるかチェックする。また、他に選択されたパラメータの妥当性が

あるかチェックしてもよい。これらの値のうちのいずれかが無効であれば、データパケットは拒絶される。これらの値が妥当であれば、STPはデータパケットを取り次ぎアクセスSCPに送信する。

高度インテリジェントネットワークへの承認されていないアクセスをさらに防止するために、本発明は、取り次ぎアクセスSCPを用いて、サービス・プロバイダーのSCP宛のデータパケットから、ある情報を除去する。この情報が除去されるのは、サービス・プロバイダーがその情報を用いてネットワークやネット

ワーク上で実行されているアプリケーションに関する不適切な情報を得ることがないようにするためである。ネットワークを通るデータパケットの経路選択を妨げることなくこの情報の除去を行うために、本発明は、取り次ぎアクセスSCPがその情報を代用情報と取り替える、ということを規定している。特に、取り次ぎアクセスSCPは、データパケットを発信したネットワーク要素によって割り当てられたトランザクション番号、発信ネットワーク要素に対応する発信点コード、および発信ネットワーク要素のサブシステム番号、に対応するデータパケット内の情報を除去する。好ましくは、第1のトランザクション番号、発信点コード、およびサブシステム番号は、データパケットの第1のトランザクション識別子を含む。第1のトランザクション識別子は、取り次ぎアクセスSCPによって記憶される。除去された情報の代用物として、取り次ぎアクセスSCPは、第2のトランザクション番号と呼ばれる乱数を生成する。これは、取り次ぎアクセスSCPとサービス・プロバイダーのSCPの間の信号経路において用いられるデータパケットと関連する。第2のトランザクション番号として乱数を用いることにより、データパケットの受領者にはネットワークの動作に関する情報が一切供給されない。取り次ぎアクセスSCPは、第2のトランザクション番号を記憶し、特に、記憶された第2のトランザクション番号は、記憶された第1のトランザクション識別子に写像される。好ましくは、取り次ぎアクセスSCPはまた、第2のトランザクション番号のあるデータパケットの受信宛先点コードを記憶する。

高度インテリジェントネットワークへの承認されていないアクセスを防止する他の方法として、本発明は、取り次ぎアクセスSCPを用いて、応答として受け取られるデータパケットの妥当性を検査する。妥当な応答については、データパ

ケットは、元々取り次ぎアクセスSCP 26' によってデータパケットに割り当てられた第2のトランザクション番号を含むべきである。データパケットがこの第2のトランザクション番号を含まない場合には、そのデータパケットは拒絶される。好ましくは、サービス・プロバイダーのSCPから受け取った応答に関して、取り次ぎアクセスSCPは、受け取ったトランザクション番号およびサービ

ス・プロバイダーのSCPのSS7の発信アドレス（または点コード）を、第2のトランザクション番号および照会であったときのデータパケットの受信宛先点コードと比較する。比較したトランザクション番号と点コードは合わねばならず、そうでない場合にはデータパケットは拒絶される。この第2の比較は、サービス・プロバイダーの応答の経路が故意でなく直接SSPへと選択されることの悪用から保護し、「不正な」SS7プロトコルの回線から保護する。受け取られた情報が記憶されている情報に対応する場合には、取り次ぎアクセスSCPは、記憶装置から対応する第1のトランザクション識別子を取得する。第1のトランザクション識別子は、取り次ぎアクセスSCPに、データパケットのさらなる経路選択または受信宛先情報を供給する。

本発明はまた、取り次ぎアクセスSCPがサービスするサービス・プロバイダーのSCPの状態の監視において取り次ぎアクセスSCPが達成する各手順によって高度インテリジェントネットワークを管理する方法を提供する。管理方法の1態様において、取り次ぎアクセスSCPは、サービス・プロバイダーのSCPが応答メッセージを戻すのにかかる時間の経過を追う。サービス・プロバイダーのSCPが応答メッセージを戻すのに、指定した最小時間よりも長く時間がかかる場合には、取り次ぎアクセスSCPは、照会メッセージを取り次ぎアクセスSCPに与えられたときに廃棄する（拒絶する、とも呼ばれる）ことによって、サービス・プロバイダーの新しいメッセージの負荷を減らす手段を講じる。本発明の管理方法の他の1態様は、取り次ぎアクセスSCPが、以前にアウトオブサービスであると決定されたサービス・プロバイダーのSCPの状態を監視する、ということである。好ましくは、取り次ぎアクセスSCPは、定期的にアウトオブサービスのサービス・プロバイダーのSCPにテストメッセージを送る。1つのテストメッセージ、または一連のテストメッセージがサービス・プロバイダーの

SCPによって正しく取り扱われる場合には、サービス・プロバイダーのSCPへの呼量は、取り次ぎアクセスSCPによって自動的に再開される。

従って、本発明の目的は、市内交換会社だけでなく、高度インテリジェントネットワークにアクセスするサービス・プロバイダーにとって、およびサービス・

プロバイダーの顧客にとって、高度インテリジェントネットワークのプライバシー、セキュリティ、および信頼性を提供することである。

また、本発明の目的は、高度インテリジェントネットワークにおいてデータパケットの呼量を取り次ぐ改良した方法を提供することである。

本発明がこれらの目的を達成し、オープンな高度インテリジェントネットワーク環境における市内交換会社の必要を満たす、ということは、以下の好適な実施例の詳細な説明から理解されるであろう。

図面の簡単な説明

図1は、それを制御する高度インテリジェントネットワークを含む、従来技術の現在の交換電話ネットワークの図である。

図2は、本発明の好適な実施例を実施する装置のブロック図である。

図3は、好適な実施例による要素間のデータパケットの流れのフローチャートである。

図4は、好適な実施例により信号中継点が行う取り次ぎ手順を示すフローチャートである。

図5は、好適な実施例により取り次ぎアクセスサービス制御点が受け取るデータパケットの取り扱いを示すフローチャートである。

図6は、好適な実施例により取り次ぎアクセスサービス制御点が行う取り次ぎ手順を示すフローチャートである。

図7は、好適な実施例により取り次ぎアクセスサービス制御点がサービスするサービス・プロバイダーのサービス制御点の状態を監視する管理方法を示すフローチャートである。

図8は、好適な実施例によるメッセージの流量の監視および管理を示すフローチャートである。

好適な実施例の詳細な説明

次に図面に移って、本発明の好適な実施例を説明する。図面では、同じ番号は同じ部品および手順を指す。図2は、好適な実施例を実施する装置のブロック図を示し、上の「発明の背景」に関連して説明した図1に示す典型的なA I Nのネ

ットワーク要素の一部を示す。

特に、図2は、2個のサービス交換点（SSP）15、15'が、関連する交換機を中継回線19bで相互接続して示されている。これらの交換機におけるSSPの論理ノードのそれぞれは、それぞれSS7データリンク21a、21bによって、信号中継点（STP）20'に接続されている。好ましくは、そして今では信頼性の目的のために普通であるが、STPはペアを組んで配置されている。従って、STP20'は、信頼性の目的のために、自らのSS7データリンクの組を有するそれぞれのSTPとのペアとして配置されている。しかし、図を簡単にするために、STPのペアのうちの1つのみ、およびSS7データリンクのうちの1組のみを図2に示す。図2において、ダッシュをつけて示して参照する番号は、前に紹介した同等物と非常に似た装置を指すが、本発明を実施するのに用いられる目的のためにある機能性が付け加えられている。図2において、本発明を実施するために、以下に図3、図4に関して説明するあるゲートウェイ・スクリーニング機能がSTP20'に付け加えられている。「ゲートウェイ」とは、通信ネットワークへの入口およびそこからの出口である。図2において、STP20'は、サービス・プロバイダーのサービス制御点（SCP）47を通るサービス・プロバイダーにとって、図1に示すような高度インテリジェントネットワーク（AIN）へのゲートウェイである。

STP20'は、SS7データリンク27を経由して、市内交換会社（LEC）が動作する取り次ぎアクセスサービス制御点（SCP）26'に接続されている。STP20'に関しては、取り次ぎアクセスSCP26'は、好ましくは、信頼性の目的のために、それぞれのペアが自らのSS7データリンクの組を有するSCPのペアとして配置されている。しかし、図を簡単にするために、SCPのペアのうちの1つのみ、およびSS7データリンクのうちの1組のみを図2に示す。取り次ぎアクセスSCP26'は、物理的に、図1に示すSCP26と同じであ

り、従って、コンピュータを有する。しかし、取り次ぎアクセスSCP26'のコンピュータは、図3、図5、および図6に関して以下に説明する好適な実施例

のある各手順を実行するためのプログラム命令を含む。取り次ぎアクセスSCP 26'のコンピュータ（別個には示していない）はまた、従来技術と同様の顧客の記録を含み、本発明を達成するためのサービス・プロバイダーの記録を含む、データベース45も有する。

STP 20'は、別のSS 7データリンク46を経由して、サービス・プロバイダーのSCP 47に接続されている。一般的に、サービス・プロバイダーのSCP 47は、何らかの交換式電話による通信サービスの形式を供給するいかなるエンティティが動作してもよい。もともと、サービス・プロバイダーのSCP 47は、そのネットワークを図1に示す市内交換会社以外のエンティティが動作するSCPを表すことが多い。図2はさらに、サービス・プロバイダーのSCP 47と現在のAINの間のインターフェースを、SS 7データリンク46に添った点48として示す。

図2に示す実施例は、以下に説明する図3ないし図5に示す各手順を実行する。高度インテリジェントネットワークのメッセージを含むデータパケットの流れを図2に関して説明し、取り次ぎ処理における各手順を図3ないし図6に関して詳細に説明する。図2の実施例における取り次ぎは、STP 20'のゲートウェイ・スクリーニング機能においてと取り次ぎアクセスSCP 26'においての両方で起こる。

一般に、図2に示す本発明の実施例において、データパケットの流れの経路は以下の2つがある。（1）SSP 15-15'から、STP 20'、取り次ぎアクセスSCP 26'、STP 20'、そしてサービス・プロバイダーのSCP 47へ、および（2）サービス・プロバイダーのSCP 47から、STP 20'、取り次ぎアクセスSCP 26'、STP 20'、そしてSSP 15-15'へ。

一般的に、発呼に関係するデータパケットは、最初第1の流れの経路をたどり、サービス・プロバイダーのSCP 47において応答が得られると、発呼に関係するデータパケットは次に第2の流れの経路をたどる。他方で、一般的に、発呼に関係しないデータパケットは、最初第2の経路をたどり、高度インテリジェント

ネットワーク要素から応答が得られると、発呼に関係しないデータパケットは次に第1の流れの経路をたどる。データパケットが発呼に関係するデータパケットにせよ発呼に関係しないデータパケットにせよ、データパケットの発信点（図2において、SSP15-15'またはサービス・プロバイダーのSCP47）が、流れの経路においてデータパケットが出会う取り次ぎ手順の組を決定する。一般的に、サービス・プロバイダーのSCP47等の市内交換会社でない発信源から発信されるデータパケットは、STP20'において主な1組の取り次ぎ手順に、そして取り次ぎアクセスSCP26'において他の主な1組の取り次ぎ手順に出会う。データパケットは他の点においても取り次ぎ手順に出会う可能性があるが、かかる取り次ぎは本明細書に説明する取り次ぎ手順と比較して含む手順が少ない、ということに注意するべきである。例えば、SSP15-15'は、AINの入メッセージのプロトコル構造を妥当とする取り次ぎ手順を含む可能性がある。しかし、SSP15-15'等のネットワーク要素から発信されるデータパケットは、取り次ぎアクセスSCP26'においてのみ主な1組の取り次ぎ手順に出会う。ネットワーク要素から発信されるデータパケットが主な1組の取り次ぎ手順にのみ出会うのは、データパケットのネットワーク発信点が高度インテリジェントネットワークのインテグリティに関して安全であると感知され、それによってSTP20'におけるさらなる取り次ぎが不要になるからである。

さらに図2を参照して、発呼に関係するデータパケットの一例を参照してこの2つの流れの経路を示す。データパケットの第1の流れの経路の創設は、SCP47と関連するサービス・プロバイダーを前もって選択しておりその加入者回線がSSP15に接続されている顧客が、自分の電話を取ってオフフックにするときに始まる。SSP15は、それに応答してトリガを生成する。このトリガは、ある特定の加入者電話番号と関連する電話がオフフックになったということを示すメッセージを含む高度インテリジェントネットワークのデータパケットである。このデータパケットは、SSP15からSS7データリンク21aを渡ってSTP20'に通される。STP20'は、データパケットの経路を、データリンク27を渡って取り次ぎアクセスSCP26'へと選択する。取り次ぎアクセスSCP26'がこのデータパケットを受け取ると、1組の取り次ぎ手順が行われ

る。

これらの手順は、図3、図5、および図6に関して以下に説明する。取り次ぎが成功した場合には、取り次ぎアクセスSCP26'はさらに、データパケットの経路をSS7データリンク27を渡ってSTP20'へと選択する。その後このデータパケットは、STP20'によって、SS7データリンク46を渡ってサービス・プロバイダーのSCP47へと転送される。

第2の流れの経路の創設は、サービス・プロバイダーのSCP47が、取り次ぎアクセスSCP26'から受け取ったデータパケットに応答してデータパケットを生成するときに始まる。この応答データパケットは、SSP15宛であり、発呼の処理において次にとるべき適切な行動に関する情報を含む。たいていの場合、次の手順は、顧客に発信音を供給するということである。サービス・プロバイダーのSCP47は、データリンク46を渡ってSTP20'に応答データパケットを送る。サービス・プロバイダーのSCP47からのデータパケットが受け取られると、STP20'は、1組の取り次ぎ手順を行う。これらの取り次ぎ手順は、図3および図4に関して以下に説明する。取り次ぎが成功した場合には、STP20'は応答データパケットをSS7データリンク27を渡って取り次ぎアクセスSCP26'に送る。応答データパケットは再び、取り次ぎアクセスSCP26'において1組の取り次ぎ手順に出会う。これらの取り次ぎ手順は、図3、図5、および図6に関して以下に説明する。この取り次ぎが成功した場合には、取り次ぎアクセスSCP26'は、応答データパケットをSS7データリンク27を渡ってSTP20'に送り、STP20'は今度は、応答データパケットをSS7データリンク21aを渡ってSSP15に送り、さらなる発呼処理が行われる。

図3および図4に関してより詳細に説明するように、STP20'がインターフェース48を横切るデータパケットを受け取ることをやめたり、サービス・プロバイダーのSCP47が適切な応答データパケットを生成することをやめるという状況が起こる可能性がある。本発明は、ネットワークがサービス・プロバイダーのSCP47と効果的に通信することができない場合には、デフォルト（d

efault)・アプリケーションを適用する。かかるデフォルト・アプリケーションがない場合には、SSP15-15'はそれらの内部のデフォルト・アプ

리케이션に完全に依存し、SSP15-15'は、それぞれのSSPと共に動作する内部のタイマのタイムアウトに応答してのみそれらのアプリケーションに進む。これらのタイマは、前に送信された出メッセージへの応答をSSPが待つ時間の量を制限する。

当業者には、デフォルト・アプリケーションの選択の範囲が広いことが明白であろう。しかし、最も普通のデフォルト・アプリケーションは、電話サービス(POTS: plain old telephone service)を設けることであろう。1実施例において、本発明は、サービス・プロバイダーが異なるデフォルトの応答を選択していない限り、すべての廃棄された最初の照会は応答メッセージの切断という結果になる、ということを規定する。オプションで、本発明は、すべての廃棄された最初の照会には取り次ぎアクセスSCP26'からの選択されたデフォルトの応答が与えられる、ということを規定する。この特定のデフォルトの応答は、発信トリガのため等の発呼処理の継続であってもよく、成端試みトリガ(terminating attempt triggers)のため等の発呼の接続であってもよく、告知を用いることであってもよく、または発呼の切断であってもよい。さらに、選択されたデフォルトの応答は、トリガ/加入者電話番号をベースにして割り当てることができてもよい。SSP15-15'からのデータパケットに適切な命令で応答するデフォルト・アプリケーションを設けることによって、高度インテリジェントネットワークを用いている発呼者がサービス・プロバイダーの側のインターフェース48の装置の故障や悪用に弱い程度がかなり低くなる。

以下の本発明の方法のフローチャートの説明に関しては、図2を参照する。

図3は、データパケットがサービス・プロバイダーのSCP47において発信されるにせよSSP15-15'等のネットワーク要素において発信されるにせよ、本発明の方法を示すフローチャートである。背景として、処理においてネットワーク要素間でのデータパケットの流れは、その流れが照会と関連する応答メッセージを1つよりも多く含んでいる場合には、会話型メッセージ・シーケンス

と呼ばれる。会話型メッセージでは、メッセージ・シーケンス（データパケット）が発呼処理において要素間を行ったり来たりして通る。メッセージ・シーケンスにおけるデータパケットは、すべてトランザクション性能アプリケーション部

（TCAP）のメッセージである。TCAPメッセージは、信号点間の回線と関係しない情報の中継に備えるSS7のサブプロトコルである。当業者には知られているように、メッセージ・シーケンスの第1のメッセージは、SS7プロトコルにおいて、照会または照会メッセージと呼ばれている。SSP15-15'等のSSPが生成するトリガは、照会の最も普通の形式である。しかし照会は、サービス・プロバイダーのSCP47等のサービス・プロバイダーのSCPによって生成されてもよい。一般的に、サービス・プロバイダーのSCPは、発呼に関係しないメッセージの場面においてのみ照会を生成する。かかる発呼に関係しないメッセージは、自動呼び出しギャップ、更新要求、変化の監視のメッセージ、およびSCPからSCPへの照会／応答メッセージを含んでもよい。

本発明において、図3のステップ100に示すように、照会を発信する要素は、照会に第1のトランザクション番号を割り当てる。トランザクション番号は高度インテリジェントネットワークにおいて既に用いられており、特に、一般的にSSPによって生成されてある特定のSSPトランザクションを識別する。第1のトランザクション番号はその発信要素にとって単一のものであるが、その番号は、高度インテリジェントネットワークの全体にわたって他の要素が生成する他のトランザクション番号と同一である可能性がある。従って、サービス制御点は、異なるSSPから発信されるが同一の第1のトランザクション番号を有するメッセージ・シーケンスを取り扱う可能性がある。しかし、図5に関して以下に説明するように、サービス制御点は、SSPから受け取った第1のトランザクション番号をそのSSPの発信点コード等の他の情報と連結することによって、メッセージ・シーケンスを識別する。

上で触れたように、照会は、発呼に関係しないメッセージの場面においてサービス・プロバイダーのSCPによって生成される可能性もある。本発明において、サービス・プロバイダーのSCP47は、現在用いられていない乱数（または

疑似乱数)を照会に割り当てることによって、第1のトランザクション番号をその照会に割り当てる。

再び図3を参照して、第1のトランザクション番号が発信要素によって生成された後、ステップ102で、第1のトランザクション番号と関連するデータパケ

ットが、STP20'等のSTPに通されて受け取られる。図2を参照して、このデータパケットがサービス・プロバイダーのSCP47から発信されている場合には、このデータパケットはSS7データリンク46を渡ってSTP20'に通される。このデータパケットがSSP15-15'から発信されている場合には、このデータパケットはそれぞれSS7データリンク21aまたは21bを渡って通される。ステップ104で、STP20'は、データパケットに関する取り次ぎが行われねばならないかどうかを決定する。上で触れたように、SSP15-15'等の高度インテリジェントネットワーク要素において発信されるデータパケットは、高度インテリジェントネットワークのインテグリティに関して安全であると知覚されるので、STP20'によって取り次ぎされない。従って、STP20'が取り次ぎを行う必要がないと決定される場合には、本方法は、以下に説明するステップ114に進む。STP20'が取り次ぎを行うと決定される場合には、ステップ106で、STP20'がかかる取り次ぎを行う。STP20'等のSTPによる取り次ぎは、図4に関して以下に説明する。ステップ108で、データパケットがSTPの取り次ぎを通ったかどうか決定される。通っていない場合には、ステップ110で、そのデータパケットは拒絶され、メッセージの拒絶後点112でルーチンから抜ける。

データパケットがSTPの取り次ぎを通っている場合には、ステップ114で、データパケットが取り次ぎアクセスSCP26'に供給されるかどうかに関して決定がなされる。供給されない場合には、ステップ110でデータパケットは拒絶され、メッセージの拒絶後点112でルーチンから抜ける。データパケットが取り次ぎアクセスSCP26'に供給される場合には、データパケットはSS7データリンク27を渡って取り次ぎアクセスSCP26'に通され受け取られる。ステップ118で、取り次ぎアクセスSCP26'は、このデータパケット

に関して取り次ぎを行う。この取り次ぎは、図5および図6に関してさらに説明する。取り次ぎの後、ステップ120で、このデータパケットが取り次ぎを通ったかどうかは決定される。通っていない場合には、ステップ110で、そのデータパケットは拒絶され、メッセージの拒絶後点112でルーチンから抜ける。図2に関して上で触れたように、好ましくは、本発明はデータパケットの拒絶に関してデ

フォルト・アプリケーションを備える。

データパケットが取り次ぎを通ると、ステップ122でデータパケットはSS7データリンク27を渡ってSTP20'に通され、次にステップ124で、STP20'がデータパケットを指定した受信宛先に通す。好ましくは、データパケットをサービス・プロバイダーのSCP47に通す前に、取り次ぎアクセスSCP26'が、サービス・プロバイダーのSCP47またはデータパケットで要求された特定のサービス・プロバイダーのサービスが使用可能状態であるということを確認する。所望のサービス・プロバイダーのSCP47または特定のサービス・プロバイダーのサービスがアウトオブサービスである場合には、取り次ぎアクセスSCP26'はデータパケットを拒絶し、適用できる場合には、上に説明したデフォルト・アプリケーションを提供する。再び図2を参照して、データパケットの受信宛先がSSP15-15'である場合には、STP20'はデータパケットをSS7データリンク21a-bのそれぞれを渡ってSSP15-15'に通す。受信宛先がサービス・プロバイダーのSCP47である場合には、STP20'はデータパケットをSS7データリンク46を渡って通す。ステップ112で、ルーチンから抜ける。

図4は、ステップ106の一部としてSTP20'が行う好適な取り次ぎ手順を示すフローチャートである。上で触れたように、取り次ぎ手順は、データパケットがサービス・プロバイダーのSCP47等の市内交換会社でないネットワーク要素から発信されている場合にのみ、STP20'によって行われる。一般的に、STP20'が行う取り次ぎ手順は、起点および受信宛先のSS7プロトコルのアドレスの妥当性検査を含む。特に、本発明は、高度インテリジェントネッ

トワークでSTPにおいて既に用いられているゲートウェイ・スクリーニング技術を用いることにより、STP 20'における取り次ぎを実施する。ゲートウェイ・スクリーニングにより、STPは、データパケット内のアドレスおよびヘッダ情報の検査と、その検査した情報のSTPが記憶している情報に関する比較をベースにして、受け取ったデータパケットを転送するかまたは拒絶する。当業者にはよく知られているように、ゲートウェイ・スクリーニングにおいて、STPは一般的に、データパケットのフィールドまたはパラメータ内の以下のタイプの

情報の1つまたはそれ以上を検査する。すなわち、発信点コード、受信宛先点コード、およびグローバル名称アドレスである。データパケット内の情報をベースにして、STPはデータパケットの経路を受信宛先情報に従って選択する。従って、従来技術においては、1つのデータパケットの経路選択の目的のために、STPは多くの異なる受信宛先を受け入れていた。しかし、本発明においては、STPは、1つのデータパケットの妥当な受信宛先として、割り当てられた取り次ぎアクセスSCPを受け入れるのみである。本発明においては、STP 20'におけるゲートウェイ・スクリーニングを用いて、サービス・プロバイダーがデータパケットの経路を、サービス・プロバイダーのSCP 47からSTP 20'および取り次ぎアクセスSCP 26'を通るように選択するよう強制する。

図4は、好適な実施例において、ステップ132でSTP 20'が、データパケット内の第1のパラメータの妥当性をチェックすることによってデータパケットの送信者を識別することを示す。特に、STP 20'は、好ましくは、データパケット内の発信点コード（送信者識別子とも呼ぶ）がサービス・プロバイダーのSCP 47のポート識別子に対応するかどうかをチェックして、データパケットの承認されたプロバイダーからそのデータパケットが受け取られたことを確認する。言い換えれば、STP 20'は、インターフェース48の物理的なポートの、SS7データリンク46上のSCPを動作することが承認されている特定のサービス・プロバイダーとの組み合わせの記録を記憶する。送信者の識別子が受領者のポート上のデータパケットの承認されたプロバイダーと対応しない場合には、そのデータパケットは1つのエンティティから発信されたことを表している

が、そのデータパケットが通ってA I Nに入ろうとしているポートのためにそのエンティティによって生成されるべきではなかったもので、S T P 2 0' がデータパケットが高度インテリジェントネットワークに入ることを許すことは不適切である。従って、発信点コードが無効の場合には、ステップ1 3 4で、データパケットは拒絶され、ステップ1 3 6でルーチンから抜ける。

発信点コードが妥当な場合には、ステップ1 3 8でS T P 2 0' がデータパケット内の第2のパラメータの妥当性をチェックする。特に、S T P 2 0' は、好ましくは、受信宛先点コード（受信宛先アドレスとも呼ばれる）を、送信者のア

イデンティティと照合する。受信宛先点コードつまり受信宛先アドレスが、サービス・プロバイダーのS C P 4 7が通信することが許されていないネットワーク要素のものである場合には、データパケットは拒絶される。特にS T P 2 0' は、好ましくは、受信宛先点コードが、S T P 2 0' の点コードに、S T P 2 0' の別名点コードに、または取り次ぎアクセスS C P 2 6' に対応するかどうかをチェックする。受信宛先点コードが無効の場合には、ステップ1 3 4でデータパケットは拒絶され、ステップ1 3 6でルーチンから抜ける。

受信宛先点コードが妥当な場合には、ステップ1 4 0でS T P 2 0' がデータパケット内の第3のパラメータの妥当性をチェックし、特に、好ましくは、サービスインジケータが妥当であるかどうかをチェックする。好適な実施例において、妥当なサービスインジケータは、メッセージ中継部（M T P）、信号接続制御部（S C C P）、またはテストメッセージに対応する。さらに、サービスインジケータのパラメータ（またはフィールド）の法定値は、米国ニュージャージー州のベルコア(BellCore)が発行した「信号システム第7の仕様書」、第T 1. 1 1 1. 4 節、T R - N W T - 0 0 0 2 4 6、第2号、第I 巻（1 9 9 1年6月）に規定されている。

好適な実施例において、ステップ1 4 0におけるチェックの結果、サービスインジケータが信号接続制御部（S C C P）に対応すると決定された場合には、ステップ1 4 2で、S T P 2 0' はあるさらなるパラメータの妥当性のチェックを継続する。特に、S T P 2 0' は、発呼者アドレス、被呼者アドレス、およびグ

ローバル名称変換をチェックする。発呼者アドレスは、法定点コード、サービス・プロバイダーのSCP47のサブシステム番号の組み合わせ、またはサービス・プロバイダーのSCP47に割り当てられた加入者電話番号(DN: Directory Number)と対応せねばならない。被呼者アドレスに関して、経路選択が点コードをベースにしておりサブシステム番号が示されている場合には、点コードは取り次ぎアクセスSCP26'のものでなければならず、サブシステム番号は取り次ぎアプリケーションプログラムのものでなければならず、グローバル名称変換が示されている場合には、被呼者アドレスのフィールド内の変換タイプは、高度インテリジェントネットワークのオープンアクセス変換のタイプでなければなら

ない。さらに、STP20'がグローバル名称変換を行う場合には、結果として得られる受信宛先点コードおよびサブシステム番号は、取り次ぎアクセスSCP26'のものでなければならず、サブシステム番号は取り次ぎアプリケーションプログラムのものでなければならず、

さらに、必要な可能性のある何らかの交互の(alternate)経路選択のために、図4に示していない他のチェックの手順をSTP20'が行ってもよい。当業者にはよく知られているように、これらの交互の経路選択の手順は、単にネットワーク内のある交換ノードか非動作であるかどうか、および交互のアドレス経路選択を用いる必要があるかどうか、を決定する処理を構成する。

図5は、取り次ぎアクセスSCP26'の受け取ったデータパケットの取り扱いを示すフローチャートである。一般的に、取り次ぎアクセスSCP26'の行う取り次ぎ手順は、取り次ぎアクセスSCP26'が受け取るSS7プロトコルのデータパケットの高度インテリジェントネットワーク部の検査を含む。ステップ148で、取り次ぎアクセスSCP26'はデータパケットを受け取る。取り次ぎアクセスSCP26'が受け取るデータパケットは、発呼に係するデータパケットであってもよく、発呼に係しないデータパケット、照会、応答メッセージ、または他の会話型メッセージであってもよい。さらに、データパケットは、サービス・プロバイダーのSCP47等のサービス・プロバイダーから受け取ってもよく、SSP15-15'等のネットワーク要素から受け取ってもよい。

データパケットを受け取った後、取り次ぎアクセスSCP 26' は、決定のステップ150を実行する。この手順で、取り次ぎアクセスSCP 26' は、データパケットが照会（照会メッセージとも呼ばれる）を含んでいるかどうか、すなわち、データパケットが新しいトランザクションまたはメッセージ・シーケンス内の第1のメッセージであるかどうか、を決定する。照会は、SSP 15-15' 等の値とワーク要素から受け取ってもよく、サービス・プロバイダーのSCP 47等のサービス・プロバイダーのSCPから受け取ってもよい。データパケットが照会を含んでいる場合、ステップ152で、取り次ぎアクセスSCP 26' は、データパケット内に含まれている情報を用いてそのデータベース45内の情報を探索し、経路を選択して、さらに発呼の処理を行う。例えば、データパケッ

トがSSP 15-15' からの照会を含んでいる場合、ステップ152で、取り次ぎアクセスSCP 26' は、データパケット内の情報を用いて、メッセージ内で識別された加入者電話番号をトリガするためのトリガを取り扱うサービス・プロバイダーのSCPを探索する。このトリガおよびトリガする加入者電話番号は、データパケットが経路選択されるサービス・プロバイダーを、単に識別する。特に、データパケットがSSP 15-15' 等のネットワーク要素から受け取られる場合には、取り次がれるアクセスSCP 26' は、好ましくは、そのデータベース45を用いてトリガする加入者電話番号／トリガのタイプのペアを、顧客が期待するサービスを供給するサービス・プロバイダーのSCPのSS7プロトコルのアドレスに写像することができねばならない。この不可欠な写像は、サービス・プロバイダーの照会を受け取る承認のチェックである。このチェックにより、サービス・プロバイダーはその顧客のためのみにデータパケットを受け取ることが保証され、それにより、すべての参加しているサービス・プロバイダーの顧客にプライバシーおよびセキュリティが保証される。従って、取り次ぎアクセスSCP 26' は、好ましくは、システム内で動作しているサービス・プロバイダーのSCPのそれぞれについてのすべての顧客の加入者電話番号のデータベース45内の情報、およびサービス・プロバイダーのSCPのそれぞれがアクセスすることが承認されているネットワーク要素に関する情報、を維持する。照会

がSCPから発信されている場合には、その照会の被呼者アドレスのフィールド内の加入者電話番号は、取り次ぎアクセスSCP26'のデータベース45への入力に合わねばならない。これによって、それぞれのサービス・プロバイダーは自身の顧客のみに影響を与える、ということが保証される。好適な実施例において、市内アクセスおよび転送領域(LATA: local access and transport area)内経路選択が用いられる場合には、サービス・プロバイダーのSCPのアドレスは、メッセージ中継部(MTP)の経路選択の点コードおよびサブシステム番号である。LATA内経路選択が必要な場合には、サービス・プロバイダーのSCPのアドレスは、ネットワーク間変換のタイプおよびグローバル名称の値である。

上で触れたように、本発明の制約のひとつは、それぞれの加入者電話番号について、それぞれのトリガは1つのサービス・プロバイダーのみを呼び出すことが

できる、ということである。従って、ステップ152で示す探索は、この特定の加入者電話番号のこの特定のトリガが、サービス・プロバイダーSCP47を通して等1つのサービス・プロバイダーにより、または図1に示すSCP26等の市内サービス制御点により市内交換会社を通して等市内交換会社により、のどちらかでサービスされ得る、ということが理解されるべきである。

取り次ぎアクセスSCP26'のデータベース45が受け取られたデータパケットのトリガに対応する情報を含んでいない場合には、ステップ153でデータパケットが拒絶され、点154でルーチンから抜ける。データベース45がかかる情報を含んでいる場合には、ステップ156で、取り次ぎアクセスSCP26'が、データベース45内のデータパケットに関連する第1のトランザクション番号、発信点コード、およびサブシステム番号を記憶する。好ましくは、第1のトランザクション番号、発信点コード、およびサブシステム番号は、そのデータパケットの第1のトランザクション識別子を含む。この第1のトランザクション識別子は、第1のトランザクション番号、発信点コード、およびサブシステム番号、の連結によって作り出される。この記憶された情報は、ステップ170-176に関して以下に説明する応答および他のメッセージの取り次ぎに関して取り

次ぎアクセスSCP26'によって求められる。

ステップ158で、取り次ぎアクセスSCP26'は、取り次ぎアクセスSCP26'とサービス・プロバイダーのSCP47の間のデータ信号経路においてまたは取り次ぎアクセスSCP26'とSSP15-15'等のネットワーク要素の間のデータ信号経路において用いられるデータパケットと関連する第2のトランザクション番号を作り出す。この第2のトランザクション番号は、データベース45内に記憶される第1のトランザクション識別子の代わりに用いられる。本発明において、取り次ぎアクセスSCP26'は、現在使わない乱数（または疑似乱数）をデータパケットに割り当てることによって、現在使わない第2のトランザクション番号をデータパケットに割り当てる。取り次ぎアクセスSCP26'は、当業者によく知られているように、疑似乱数ジェネレータから乱数を取得する。「現在使われていない」乱数とは、ネットワークを通して、進行中のデータパケットに割り当てた乱数の経過を取り次ぎアクセスSCP26'が追って

いる、ということを意味する。取り次ぎアクセスSCP26'は、データパケットに乱数を割り当てる前にそのデータベース45内のリストまたはテーブルに情報を求め、選択された乱数が進行中のデータパケットの乱数と重複しないということが確認される。

好ましくは、取り次ぎアクセスSCP26'は、割り当てられた第2のトランザクション番号を、データベース45内の上記リストまたはテーブル内に記憶する。乱数をデータパケットの第2のトランザクション番号として用いることにより、第2のトランザクション番号が決して第1のトランザクション番号と相関していないということが確かめられる。このようにして、第2のトランザクション番号は、データパケットの受領者に何ら情報を与えない。乱数を第2のトランザクション番号として用いることにより、メッセージの発信者が、ライバルが用いるようなトランザクション番号を計算してライバルの顧客の発呼を制御しようとすることが防止される。また、このように乱数を用いることによって、メッセージの発信者が自身の発呼に割り当てられたトランザクション番号を分析することによってライバルの発呼に割り当てられたトランザクション番号を推測することも

防止される。

取り次ぎアクセスSCP26'が第2のトランザクション番号を作り出した後、ステップ160で、取り次ぎアクセスSCP26'は、データベース45内に、第1のトランザクション識別子への第2のトランザクション番号の写像を維持する。好適な実施例で、取り次ぎアクセスSCP26'はまた、第2のトランザクション番号を、データパケットの受信宛先点コードと関連するデータベース45内のテーブルに入力する。データパケットの受信宛先がサービス・プロバイダーのSCP47である場合には、受信宛先点コードは、サービス・プロバイダーのSCP47の点コードである。さらに、好適な実施例は、データパケットの受信宛先点コードを第2のトランザクション番号と関連づけ、この情報の組み合わせの写像を第1のトランザクション識別子に維持する。さらに、SCPから発信されるメッセージに関して、取り次ぎアクセスSCP26'は、最初のメッセージの被呼者のアドレスのフィールド内の加入者電話番号を、目標ネットワーク要素の受信宛先点コードおよびサブシステム番号に写像せねばならない。これによつ

て、受信宛先加入者が実際にサービス・プロバイダーの顧客であることが保証される。

ステップ162で、取り次ぎアクセスSCP26'は、データパケットから第1のトランザクション識別子に対応する情報を取り去り、ステップ164で、取り次ぎアクセスSCP26'は、第2のトランザクション番号をデータパケットに用いる。かかる代用によって、データパケットから何らかの通信トランザクション情報を得ることが、不可能ではないにしても困難になるので、第2のトランザクション番号を第1のトランザクション識別子の代用とすることによって、高度インテリジェントネットワークのインテグリティは維持される。第1のトランザクション識別子を取り去って第2のトランザクション情報を代用した後、ステップ166で修正されたパケットはその受信宛先に送られ、点168でルーチンから抜ける。

再びステップ150を参照して、受け取られたデータパケットが照会ではない

場合には、データパケットは応答（応答メッセージまたは会話型メッセージとも呼ばれる）に相当する。妥当な応答つまり会話型メッセージについては、データパケットは、元々取り次ぎアクセスSCP26'が割り当てた第2のトランザクション番号を含むべきである。従って、ステップ170で、取り次ぎアクセスSCP26'は、トランザクション番号を応答データパケットと関連して比較し、トランザクション番号をデータベース45内で維持されている活動状態の第2トランザクション番号のリストと比較する。

好適な実施例において、サービス・プロバイダーのSCP47から受け取る応答に関して、取り次ぎアクセスSCP26'は、別の比較を行う。取り次ぎアクセスSCP26'は、応答内のある情報を、応答メッセージに対応する照会を受け取る結果として記憶されたデータベース45内のある情報と比較する。特に、取り次ぎアクセスSCP26'は、応答内の以下の情報—受け取られたトランザクション番号およびサービス・プロバイダーのSCP47のSS7の発信アドレス（または点コード）—を、データベース45内の以下の情報—データパケットの第2のトランザクション番号および照会であったときの受信宛先点コード—と比較する。比較されたトランザクション番号と点コードは、好ましくは、継続さ

れる取り次ぎについて合わねばならない(match for)。サービス・プロバイダーのSCP47と関連するトランザクション番号間および点コード間の対応を必要とするということを含む、好適な実施例の二重のチェックによって、本発明は、明らかな利点を提供する。この二重チェックシステムは、サービス・プロバイダーの応答の経路が故意でなく直接SSPへと選択される（例えば、市内交換会社のSTPの経路選択テーブルにおけるエラーのために）ことの悪用から保護し、「不正な」SS7プロトコルの回線から保護する。

再び図5を参照して、ステップ172で、取り次ぎアクセスSCP26'は、上に説明したように受け取られたデータパケットと関連する情報がデータベース45内の情報と対応しているかどうかをチェックする。そうでない場合には、対応していないということは、無効なトランザクション番号を用いた高度インテリジェントネットワーク要素から照会でないメッセージが受け取られた、というこ

とを意味する。この場合には、ステップ173でデータパケットは拒絶され、ステップ174でルーチンから抜ける。

受け取られた情報が記憶されている情報と対応する場合には、ステップ176で、取り次ぎアクセスSCP26'はデータベース45から受け取られた(第2の)トランザクション番号に対応する第1のトランザクション識別子を取得する。第1のトランザクション識別子呼び出すと、取り次ぎアクセスSCP26'は、そのデータパケットのさらなる経路選択または受信宛先の情報を取得する。この受信宛先情報は、点コードおよびサブシステム番号、またはネットワーク間の変換のタイプおよびグローバル名称の値を含んでもよい。取り次ぎアクセスSCP26'は、受け取られたデータパケットからそのアドレス情報を取り去り、データベース45から取得した受信宛先情報を加え、そのデータパケットがSSPその他以前のデータパケットが発信された要素へ戻されるようにする。ルーチンは進んで、ステップ166で修正されたパケットを送り、ステップ168で抜ける。

1実施例において、本発明はさらなる比較または妥当性検査の手順を行い、応答データパケットがトランザクションを開始したデータパケットと対応するということを決定する。これらのさらなる妥当性検査の手順は、それぞれの応答TCP APメッセージのアンパックおよび特定のパラメータの値のそれぞれの検査を含

み、パラメータの値が最初のデータパケット内の対応する特定のパラメータの値と対応するということを決定する。最初のデータパケット内には存在していなかったり、あるいはその値がサービス・プロバイダーによって変えられたパラメータについてのみ、取り次ぎ手順が必要である。従って、応答データパケットのパラメータの値における、最初のデータパケット内のパラメータの値からの変化の検査を行うために、取り次ぎアクセスSCP26'は、最初のデータパケットのパラメータの値の記録を、データベース45内に維持している。

図6は、ある特定のタイプの高度インテリジェントネットワークのメッセージについて好適な実施例が実行する取り次ぎのプロセスを示す。図示の各手順は取り次ぎアクセスSCP26'が実行する、ということが理解されるべきである。

承認されたアクティビティに関する照会は、データベース 4 5 (図 2) 内の様々なテーブル内に記憶されている。この部分の取り次ぎ処理がステップ 1 8 0 で入力され、ここで取り次ぎアクセス S C P 2 6' がデータパケットを受け取る。ステップ 1 8 2 で、取り次ぎアクセス S C P 2 6' が、データパケット内の特定の中継回線のグループの経路選択の何らかの要求があるかどうかをチェックする。何らかの中継回線のグループが要求されない場合には、妥当な中継回線のグループの要求 1 8 6 の周囲にループを描く N O の枝路 1 2 6 を通ってステップ 1 8 8 へと進む。1 個またはそれ以上の中継回線のグループが要求される場合には、ステップ 1 8 6 で、取り次ぎアクセス S C P 2 6' が、そのデータパケットを生成したサービス・プロバイダーの、およびそのデータパケットが向かう S S P の、法定の中継回線のグループのルートインデックスのテーブルをチェックする。

妥当な中継回線のグループのこのテストは、要求内で指定されたそれぞれの中継回線のグループについて行われる、というのも、その代わりに用いることのできる多数の中継回線のグループを中継回線のグループの経路選択の要求において指定してもよいからである。要求された中継回線のグループのうちのいずれか 1 個でもこのサービス・プロバイダーの S C P による使用が承認されていない場合には、ステップ 1 8 6 から N O の枝路へと進み、これは、ステップ 1 8 7 A におけるデータパケットの拒絶、ステップ 1 8 7 B (オプション) におけるデフォルト・アプリケーションの供給、およびステップ 1 8 7 C におけるルーチンからの

抜け、に通じる。サービス・プロバイダーの S C P が中継回線のグループの経路選択の要求に含まれるそれぞれの中継回線のグループを用いることが承認されている場合には、処理は次の手順であるステップ 1 8 8 へと進む。

好適な実施例は、承認されていない中継回線のグループを用いる可能性のある何らかの要求が検出される場合にはメッセージを拒絶する、ということに注目するべきである。取り次ぎアクセス S C P にデータパケットを再構成させて、承認されていない中継回線のグループは削除するがサービス・プロバイダーの S C P が用いることを承認されている 1 個またはそれ以上の中継回線のグループは含むようにすることも可能である。しかし、中継回線のグループの経路選択の適切な

要求をするという責務は、サービス・プロバイダーに負わせることが好ましいと考えられる。

ステップ188で、データパケットがテストされ、交換機でない高度インテリジェントネットワーク要素へのアクセスが要求されているかどうかが確かめられる。上で触れたとおり、ある特定の加入者電話番号への発呼に影響を与えることへの承認は、その加入者電話番号を取り扱う交換機と関連するSSPと通信することへの承認を暗示している。しかし、他のサービス制御点またはサービス接続点等の交換機でない高度インテリジェントネットワーク要素へのアクセスを求めたデータパケットについての別個のテストが含まれている。

これまでのテストと同様、交換機でない高度インテリジェントネットワーク要素が要求されている場合には、ステップ188から承認のテスト190の周囲にループを描くNOの枝路を通してステップ192へと進む。メッセージの要求が交換機でない高度インテリジェントネットワーク要素へのアクセスの要求を含む場合には、YESの枝路を通してステップ190へと進み、ここで加入者電話番号のテーブルが情報を求められてその交換機でない高度インテリジェントネットワーク要素の加入者電話番号がこの特定のサービス・プロバイダーのSCPの承認された加入者電話番号のリストに含まれているかどうかが決定的である。従来は交換機ではない高度インテリジェントネットワーク要素に割り当てられてきた交換機でない要素の指定を、その加入者電話番号で記憶するのが好ましい、ということに注目するべきである。加入者電話番号は、交換機でない要素を指定する好

適な方法である。これにより、サービス・プロバイダーがSS7の点コードを知ったり用いる必要がなくなることにより、ネットワークのセキュリティがさらに与えられる。この場合、加入者電話番号は、ステップ152（図5）に関して上に説明した加入者電話番号の妥当性検査と同様に、ある特定の加入者回線または加入者専用中継回線に関連する加入者電話番号なのではない、ということに注目するべきである。

再びステップ190を参照して、サービス・プロバイダーのSCPが要求されている交換機でない高度インテリジェントネットワーク要素にアクセスすること

を承認されていない場合には、NOの枝路へと進み、これは、ステップ187Aにおけるデータパケットの拒絶、ステップ187B（オプション）におけるデフォルト・アプリケーションの供給、およびステップ187Cにおけるルーチンからの抜け、に通じる。サービス・プロバイダーのSCPが承認されている場合には、YESの枝路からステップ192へと進む。ステップ192で、チェックが行われ、データパケットが限られた資源の使用を求めているかどうかを決定する。好適な実施例は、限られた資源というものを、ある限られた数存在し、いかなる与えられたサービス・プロバイダーによって占有される時間をも厳密に制御する必要がある、少なくとも1個のクラスのネットワーク資源である、と定義する。本明細書において用いる概念では次のようには限定しないが、限られた資源というのは、通常、リアルタイムの発呼への音声接続に関係し発呼者から供給されるかまたは発呼者に送られるかのどちらかの音声信号のある形式を処理する装置である。かかる装置に共通の特性は、使用されるとき毎に比較的長時間用いられる、ということである。好適な実施例においては、交換ディジット受信機および音声による告知の装置が、限られた資源として分類される。しかし、本発明の他の実施例では、他の装置を限られた資源として分類してもよく、実際、本発明の実施について定義される多数の階層的クラスの資源があり得る。

限られた資源が何ら要求されない場合には、取り次ぎのテストのパスに成功し、NOの枝路へと進み、ステップ184でルーチンから抜ける。限られた資源が要求されている場合には、YESの枝路からステップ194へと進む。この手順は、サービス・プロバイダーのSCPがこの資源またはこの資源のクラスを用いるこ

とを承認されているかどうかをテストするものである。このテストに添わなければ、NOの枝路に進みステップ184でルーチンから抜ける。再びステップ194を参照して、サービス・プロバイダーのSCPが資源を用いることを承認されている場合には、YESの枝路からステップ196へと進む、ステップ196で好適な実施例の重要な取り次ぎ機能がテストされる。好適な実施例が限られた資源として定義するネットワーク資源のクラスは通常用いられる毎に長時間占有さ

れる装置を含むので、好適な実施例の方法は、与えられたサービス・プロバイダーが同時に占有することのできるかかる装置の数に制限を設けている。この上限を資源占有数と呼び、これは単に、サービス・プロバイダーまたはそのアプリケーションが同時に占有してもよい限られた資源の装置の所定の数である。

資源占有数は、収容できるサービス・プロバイダーの数からの最大許容数によってのみ選択するのではなく、料金に応じて決めるのが好ましいと思われる。従って、音声による告知装置を大量に用いると予想するサービス・プロバイダーは、それらの資源へのアクセスを設けることについて市内交換会社により高い料金を払って、比較的多数のそれらの資源を同時に占有することができるようにする必要がある。

限られた資源または資源のクラスの総数の代わりに、またはそれに加えて用いてもよい、資源占有数を定義する他の方法もある。特に、ひとつのサービスが占有する限られた資源の総数のみでなく、与えられた資源の所有者における、すなわち与えられた交換機または与えられたサービス接続点における限られた資源の総数も制限する、ということが重要である。例えば、あるサービス・プロバイダーのSCPがアクセスしてもよいある特定のサービス接続点に5本の音声による告知の回線がある場合、ひとつのサービス・プロバイダーのSCPが同時に5本全部の回線を占有してネットワーク上で実行されている他のアプリケーションに音声回線を提供することを妨げることはできない、ということを確認することが重要である。これは、本発明の実施例における資源占有数に特有の定義となりうる。さらに、サービスのアプリケーションが、ネットワーク内の様々な資源の所有者の中でその数の限られた資源よりも多くを占有することが許されている場合であっても、これをさらなる制限として指定してもよい。

本発明の方法は、好ましくは、ひとつのサービス・プロバイダーのアプリケーションが同時に占有してもよい限られた資源の数の所定の上限である資源占有数を規定する。このシステムは、それぞれのサービス・プロバイダーのアプリケーションについての数が増える方向／減る方向へのカウントとして、限られた資源のカウントを維持する。ステップ196に達すると、取り次ぎアクセスSCP2

6' は、このサービス・プロバイダーについての限られた資源のカウン트가現在資源占有数を超えているかどうかをテストする。このテストが真である場合、YESの枝路へと進み、これは、ステップ187Aにおけるデータパケットの拒絶、ステップ187B（オプション）におけるデフォルト・アプリケーションの供給、およびステップ187Cにおけるルーチンからの抜け、に通じる。限られた資源の使用を要求する顧客にサービスを提供するために、リトライの試み等の問題に取り組むことは、サービス・プロバイダーの義務である。

限られた資源のカウン트가まだ資源占有数よりも小さい場合には、ステップ196からNOの枝路をとってステップ198へと進み、ここで限られた資源のカウン트가インクリメントされる。ステップ198の後、処理は進んで、ステップ199でルーチンから抜ける。

図示していない会話の終了を取り扱う他のルーチンには、その特定のサービス・プロバイダーが要求する限られた資源のユーザが完了したときにはいつでも限られた資源のカウン트를デクレメントする責任がある、ということに注目すべきである。数が増える方向／減る方向へのカウン트의体系の実施は、当業者には簡単でありよく知られている。

1 実施例において、本発明は、少なくとももう1つの妥当性検査または取り次ぎ手順を行う。特に、取り次ぎアクセスSCP26' は、料金番号および交互のビルギン番号に対応する応答データパケット内のパラメータの値に関して気付かれる変化を検査する。料金番号にまたは交互のビルギン番号に対応する応答データパケット内のパラメータの値が最初のデータパケット内の値から変化する場合には、取り次ぎアクセスSCP26' が、変化した値（料金番号、交互のビルギン番号、あるいはその両方）を、サービス・プロバイダーの顧客の加入者電話番号のリストに関するデータベース45内の情報と比較する。変化した値と加入者

電話番号のリストの間に符合が見つからない場合には、取り次ぎアクセスSCP26' は、応答データパケットを拒絶する。

本発明はまた、取り次ぎアクセスSCP26' がサービスするサービス・プロバイダーのSCPの状態の監視において取り次ぎアクセスSCP26' が達成す

る各手順によってネットワークを管理する方法を提供する。この管理方法の1様は、取り次ぎアクセスSCP 26'が、サービス・プロバイダーのSCPが応答メッセージを戻すのにかかる時間の経過を追う、というものである。サービス・プロバイダーのSCPが応答メッセージを戻すのに、指定した最小時間よりも長く時間がかかる場合には、取り次ぎアクセスSCPは、メッセージのいくつかを廃棄することによって、サービス・プロバイダーの新しいメッセージの負荷を減らす手段を講じる。サービス・プロバイダーが、廃棄されるメッセージのデフォルト・アプリケーションを指定している場合には、取り次ぎアクセスSCPは、好ましくは、かかるデフォルト・アプリケーションをそれぞれの廃棄されるメッセージに供給する。取り次ぎアクセスSCPがデフォルト・アプリケーションを供給しない場合には、交換機は、例えば電話サービス(POTS)等の標準のデフォルト処理をしてメッセージを供給する。

図7は、取り次ぎアクセスSCP 26'にサービスされるサービス・プロバイダーのSCP 47の状態を監視する管理方法を示すフローチャートである。ステップ200で、取り次ぎアクセスSCP 26'は、データパケットの経路をサービス・プロバイダーのSCP 47へと選択し、ステップ202で、取り次ぎアクセスSCP 26'は、サービス・プロバイダーのSCP 47が応答メッセージを戻すのにかかる時間の量に関するタイマをスタートさせる。決定のステップ204で、取り次ぎアクセスSCP 26'は、タイマが切れたかどうかをチェックする。このタイマーの値は、好ましくは、スイッチタイマ(switch timer)よりも約2秒小さい値に設定されている。タイマが切れていない場合には、NOの枝路をとって、タイマが切れるまでタイマが切れたかどうかをチェックする手順を繰り返す。いったんタイマが切れると、ステップ206で、取り次ぎアクセスSCP 26'が、応答が受け取られたかどうかをチェックする。そうである場合には、ステップ208でルーチンから抜ける。応答が受け取られていない場合には、ステ

ップ210で、取り次ぎアクセスSCP 26'が、サービス・プロバイダーがデフォルト処理またはアプリケーションが供給されるよう指定したかどうかをチェックする。そうである場合には、ステップ212で、取り次ぎアクセスSCP 2

6' が、指定されたデフォルト処理を供給する。サービス・プロバイダーがデフォルト処理を供給していない場合には、ステップ 212 のデフォルト処理の供給の周囲にループを描くステップ 210 の NO の枝路をとって、ステップ 216 へ進む。ステップ 216 で、取り次ぎアクセス SCP 26' は、サービス・プロバイダーの SCP のメッセージの負荷を減らすべきかどうかをチェックする。サービス・プロバイダーの SCP のメッセージの負荷を減らす決定は、上に説明したタイマ機能によって供給される情報をベースにした予め選択した時間の期間内に 1 つまたはそれ以上の応答メッセージを戻せないということを含む、様々な要因をベースにしてもよい。メッセージの負荷が減らされるべきでない場合には、ルーチンは進んでステップ 208 で抜ける。メッセージの負荷が減らされるべき場合には、ステップ 218 で、取り次ぎアクセス SCP 26' は、サービス・プロバイダーの SCP 47 に向けられた次の新しい照会を廃棄することによってメッセージの負荷を減らすことに進む。前と同様、サービス・プロバイダーがデフォルト処理を指定している場合には、ステップ 220 で、取り次ぎアクセス SCP 26' が、廃棄された新しい照会にかかるデフォルト処理を供給する。指定したデフォルト処理の供給の後、ルーチンはループを描いて決定のステップ 216 に戻り、サービス・プロバイダーの SCP のメッセージの負荷が減らされるべきかどうかをチェックする。サービス・プロバイダーの SCP のメッセージの負荷を減らす交互のまたはさらなる手段は、負荷のかかりすぎたサービス・プロバイダーの顧客に役立っている SSP 15-15' 等の SSP に、取り次ぎアクセス SCP 26' によって自動発呼ギャッピング (ACG : Automatic Call Gapping) のメッセージを供給することである。好ましくは、取り次ぎアクセス SCP は、メッセージの流量を監視し、特に、取り次ぎアクセス SCP がサービスするサービス・プロバイダーが用いるそれぞれの終端トリガ・メッセージの流量を監視する。取り次がれた SCP が、サービス・プロバイダーの SCP が負荷がかかりすぎになっているということを検出する場合には、取り次ぎアクセス SCP は、負

荷のかかりすぎたサービス・プロバイダーの顧客に役立っている SSP に、自動発呼ギャッピングのメッセージを送る。負荷を減らしてもタイミングの問題が解

決されない場合には、取り次ぎアクセスSCPは、サービス・プロバイダーのSCPがアウトオブサービスであると決定する。サービス・プロバイダーのメッセージの負荷が減らされるべきではないと決定されるまでステップ216～220が繰り返され、ステップ208でルーチンから抜ける。

本発明の管理方法の他の1態様は、取り次ぎアクセスSCPが、以前にアウトオブサービスであると決定されたサービス・プロバイダーのSCPの状態を監視する、ということである。好ましくは、取り次ぎアクセスSCP26'は、定期的に（1分間に1回等）アウトオブサービスのサービス・プロバイダーのSCPにテストメッセージを送る。1つのテストメッセージ、または一連のテストメッセージがサービス・プロバイダーのSCPに正しく取り扱われる場合には、サービス・プロバイダーのSCPへの呼量は、取り次ぎアクセスSCP26'によって自動的に再開される。

さらに、本発明はまた、メッセージの失敗に関するセキュリティの監査証跡の維持にも備える。取り次ぎの失敗および高度インテリジェントネットワークのメッセージの失敗（プロトコルのエラー、拒絶、戻りのエラー、アプリケーションのエラー、等）はすべて、監査できる事象であると考えられる。監査できる事象には、トランザクションを確立しようとする無効な試み、データにアクセスしようとする無効な試みについてのすべての記録、およびセキュリティ処理の構成のすべての変化、を含む。それぞれの監査できる事象について、監査証跡は、日付、時間、含まれるTCPメッセージ（MTPおよびSCCPのデータを含む）の写し、トリガのタイプおよびトリガする受信宛先番号、および何らかのエラーコード、を含む。本発明において、監査証跡の概念は、高度インテリジェントネットワーク維持パラメータの概念と類似するものとして考えられている。1実施例において、本発明は、受け取るネットワーク要素に、付属のデータパケットのセキュリティの監査を作動させるように要求する、データパケット内のパラメータを含む。セキュリティ・パラメータは、単一の識別子の役割をし、異なるネットワーク要素からの監査の記録をリンクすることによって、監査されるユーザがと

る行動の、ネットワークの広い視野を得ることができるようになっている。セキュリティ・パラメータは、アクセスの失敗を繰り返した後トランザクションが確立したり、通常昼間にのみ操作するユーザが夜間にトランザクションを確立する、等の、普通でないセキュリティの事象が起こるときに作動してもよい。

本発明の管理方法の他の1態様は、取り次ぎアクセスSCPが、サービス・プロバイダーのSCPの選択された加入しきい値に従って、およびネットワークの容量に従って取り次ぎアクセスSCPが役立つサービス・プロバイダーのSCPに入ってくる方とそこから出ていく方の両方のメッセージの流量を監視し管理する、というものである。特に、サービス・プロバイダーのSCP47は、メッセージの流量に関して加入しきい値を与えられている。取り次ぎアクセスSCP26'は、サービス・プロバイダーのSCPへのメッセージの流れが、少なくともネットワークのメッセージの呼量をベースにした加入しきい値に達するのを許す。サービス・プロバイダーのSCP47へのメッセージの流量が加入しきい値を超える場合には、メッセージの経路をサービス・プロバイダーのSCP47へと選択することを継続するかどうかを決定するために、取り次ぎされたSCP26'がネットワークのメッセージの呼量を評価する。取り次ぎアクセスSCP26'がその容量を有する場合には、好適な実施例において、取り次ぎアクセスSCP26'は、メッセージの流量の加入しきい値を超えていても、メッセージの経路をサービス・プロバイダーのSCP47へと選択することを継続する。取り次ぎアクセスSCP26'に負荷がかかりすぎている場合には、サービス・プロバイダーSCP47への照会を拒絶する（応答メッセージとは対照的に）。拒絶されたメッセージのデフォルト・アプリケーションをサービス・プロバイダーのSCP47が選択している場合には、取り次ぎアクセスSCP26'がデフォルト・アプリケーションを用いる。

取り次ぎアクセスSCP26'のメッセージの負荷を減らす交互のまたはさらなる手段は、SSP15-15'等のSSPに、取り次ぎアクセスSCP26'によって自動発呼ギャッピング（ACG）のメッセージを供給することである。好ましくは、以下に図8に関して説明するように、取り次ぎアクセスSCP26'は、メッセージの流量を監視し、特に、取り次ぎアクセスSCP26'がサー

ビスするサービス・プロバイダーが用いるそれぞれの終端トリガ・メッセージの流量を監視する。取り次ぎアクセスSCP 26' が負荷がかかりすぎになっているということを検出する場合には、取り次ぎアクセスSCP 26' は、取り次ぎアクセスSCP 26' が役立っているサービス・プロバイダーの顧客に役立っているSSPに、自動発呼ギャッピング（ACG）のメッセージを送る。

図8は、本発明の流量の監視および管理を示すフローチャートである。ステップ240でデータパケットを受け取ると、ステップ242で、取り次ぎアクセスSCP 26' が、送信者の識別子のデータパケットの適切なフィールドをチェックする。送信者の識別子は、そのメッセージを作り出したエンティティを識別するコードである。ルーチン244において、ステップ242で識別された送信者と関連する現在のカウン트가インクリメントされ、適切なタイマの値が記憶される。これらのカウン트는、いくつかの目的のために維持される。そのひとつは、第三者のサービス・プロバイダーに高度インテリジェントネットワークの使用について課金するためにある特定の送信者が生成する照会／応答のペアのカウン트를維持する、ということである。さらに、サービス・プロバイダーの動作しているSCP 47からインターフェース48を横切ってパケットメッセージが供給される入メッセージの流量が計算される。この入メッセージの流量は、比較的短期間にわたる平均である。さらに、過度のメッセージ呼量の警告状態が検出できるように、より長期間の平均が維持される。好適な実施例においては、所定の値を超える短期間の入メッセージの流量のみによって、インターフェース48がブロックされる。

ステップ246で、計算した入メッセージの流量が、その特定のサービス・プロバイダーの承認されたメッセージの流量数と比較される。この数は、取り次ぎアクセスSCP 26' 内のデータベース45内のサービス・プロバイダーの記録内に記憶されている。確立された判定基準によって入メッセージの流量が過剰である場合には、YESの枝路からルーチン248へと進み、ここで、取り次ぎアクセスSCP 26' によって、サービス・プロバイダーのSCP 47に通知するメッセージが、インターフェース48を横切って送信し戻される。これによって、サービス・プロバイダーのSCPは、示したものよりも大きいインターフェー

48を横切るメッセージを送信する流量が用いられる場合には、とることのできる何らかの適切な行動をとることができる。

ここから、ルーチンは決定のステップ250へと進み、ここで入メッセージの流量が承認されたメッセージの流量を超えている程度がチェックされる。入メッセージの流量が、少なくともネットワークが他のサービス・プロバイダーに適切にタイムリーにサービスを提供することのできる能力が損なわれる等の所定の量だけ、承認されたメッセージの流量数を超えている場合には、取り次ぎ処理は、物理的なポートおよびブロックのインターフェース48を横切るメッセージの動きを終了する。このオプションが要求される場合には、ステップ250からYESの枝路へと進む。反対に、入メッセージの流量は大きすぎるがネットワークの性能をひどく低下させるほど過剰ではない場合には、ステップ250からNOの枝路へと進む。

最初に、入メッセージの流量が、少なくとも上述の所定の量だけ承認されたメッセージの流量数を超えている状況を考える。論理はステップ252へと進み、ここで、STP20'に終了のメッセージが送られる。これは、STPに、インターフェース48を横切る入呼量を終了するように、従ってそれによって表される物理的なポートをブロックするように、命令する。次に、ステップ254に達し、ここでSCPは、サービス管理システム（図1）に、SS7データリンク46のポート48におけるアクセスの終了を通知する。これによって、サービス管理システムにおける人員は、そのアクセスが遮断されているサービス・プロバイダーにコンタクトをとって、是正処置をとることができるかどうか調べる機会が与えられる。さらに、これによって、この特定のサービス・プロバイダーの顧客から苦情があるかもしれないということを見越して、サービス管理システムに終了が通知される。

ステップ256で表されるルーチンは、上で説明したデフォルト・アプリケーションの起動である。図2の実施例における、パケットメッセージを行ったり来たりして通すパターンへの説明より、デフォルト・アプリケーションの一部は

電話局（SSP）15-15'の1つ内で発信されるパケットに応答してSCP 26'からSS7データリンク46にパケットを送る処理を終了することである、

ということが理解される。従って、取り次ぎアクセスSCP 26'は、通常に取り次ぎ機能を行ってその後パケットをサービス・プロバイダーのSCP 47へと送るのではなく、通常はサービス・プロバイダーのSCP 47に送られる受け取られたパケットにどんな応答をデフォルト・アプリケーションが与えるかに関して、決定を行わねばならない。従って、いったんこの状態に入ると、最終的にサービス・プロバイダーのSCP 47向けに意図されたパケットに応答して取り次ぎアクセスSCP 26'が外へ送信するその特定のパケットはSCP 26'上で実行されているデフォルト・アプリケーションに従って修正され、インターフェース48のブロッキングがクリアされるまでこの状態が優勢である（prevail）、ということが理解されるべきである。従って、ステップ246で用いられるテストの一部は、インターフェース48が既にブロックされているかどうかを決定することである、ということが理解されるべきである。そのような場合には、終了命令を出し続けることは無駄である。

いったんデフォルト・アプリケーションが起動すると、次のパケットが受け取られるまで、ステップ258でルーチンから抜ける。

次に、ステップ250からNOの枝路へと進む状況を考える。まず、決定のステップ260が実行され、ここでメッセージを拒絶する判定基準が調べられる。判定基準には、入メッセージの流量が承認されたメッセージの流量数を超える程度、およびメッセージ自体の性質、が含まれる。後者を考えた場合に関し、メッセージは、単に拒絶されその向けられた受信宛先に送られない場合には、顧客の電話をサービスを供給することができない状態にロックしたままにする可能性のあるものであるかもしれない。ステップ260の決定がベースにすることができる他の判断基準もある。メッセージが拒絶されないと仮定すると、NOの枝路へと進み、ステップ248でルーチンから抜ける。

メッセージが拒絶される場合には、ステップ260からYESの枝路をとり、

ステップ262へと進む。この手順で、拒絶メッセージが送信者、今考えている例ではサービス・プロバイダーのSCP47、に送信される。メッセージの拒絶は、他のネットワーク要素、特に電話局の交換機におけるSSP、の動作に悪影響を及ぼす可能性があるので、ステップ264で、サービス・プロバイダーから

メッセージを拒絶した結果としてエラーメッセージを生成するべきかどうかに関して決定がなされる。これが適切であるとみなされる場合には、YESの枝路からステップ266へと進み、ここで、SCP47が応答しようとしていた元々のメッセージを送ったSSPにエラーメッセージが送られる。ここから、ステップ268でルーチンから抜ける。エラーメッセージが必要でない場合には当然、ステップ264からNOの枝路へと進み、ステップ268で直接ルーチンから抜ける。

ステップ248と268の間の各手順の説明は、この方法の論理がステップ246で過剰な入メッセージの流量を検出したという過程をベースにした。入メッセージが過剰でない場合には、ステップ246からNOの枝路へと進み、ステップ270で直接ルーチンから抜ける。

前述のことから、本明細書で説明した方法によって、サービス・プロバイダーのSCPと取り次ぎアクセスSCPの間の取り次がれたインターフェースを横切る効果的な取り次ぎが行われる、ということが理解されよう。第1および第2のトランザクション番号を用いることにより、市内交換会社によるネットワークの動作に関する機密に関わる情報へのアクセスやサービス・プロバイダーのライバルに関する情報にアクセスする可能性からサービス・プロバイダーを効果的に分離する。図示の取り次ぎの各手順により、サービス・プロバイダーが生成するメッセージのインテグリティが保証される。さらに、図示の取り次ぎの各手順により、サービス・プロバイダーに与えられ市内交換会社にかかる特権のサポートのために費用を費やさせる高度インテリジェントネットワーク内のある特権の料金を市内交換会社が定めることが強制される。この強制により、いかなる特定のサービス・プロバイダーが、他のサービス・プロバイダーの顧客の不利益になったり市内交換会社の不利益になるようにそのネットワーク内でのあるタイプの資源

の割合が極端に固定することも、防止される。

好適な実施例の前述の説明より、当業者には本発明の他の実施例も示唆され、従って、本発明の範囲は以下の請求の範囲およびその均等物によってのみ限定されねばならない。

【図1】

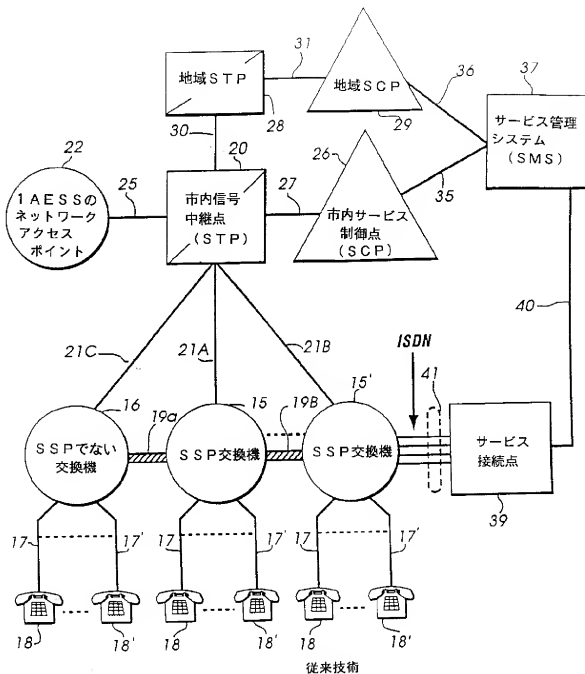


FIG 1

【図 2】

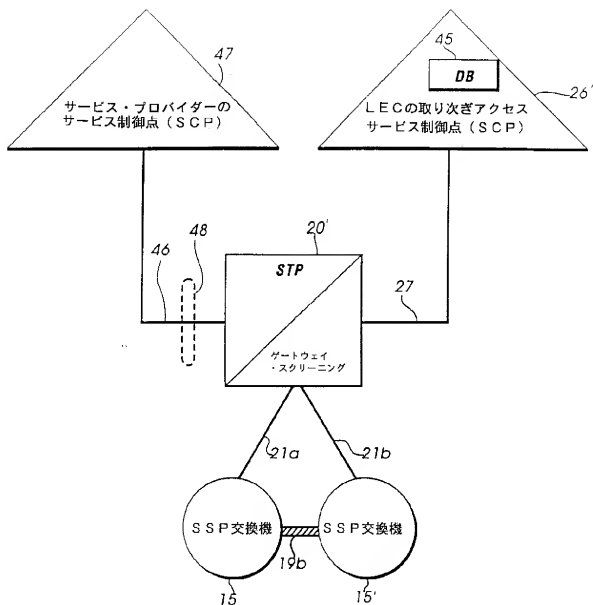


FIG 2

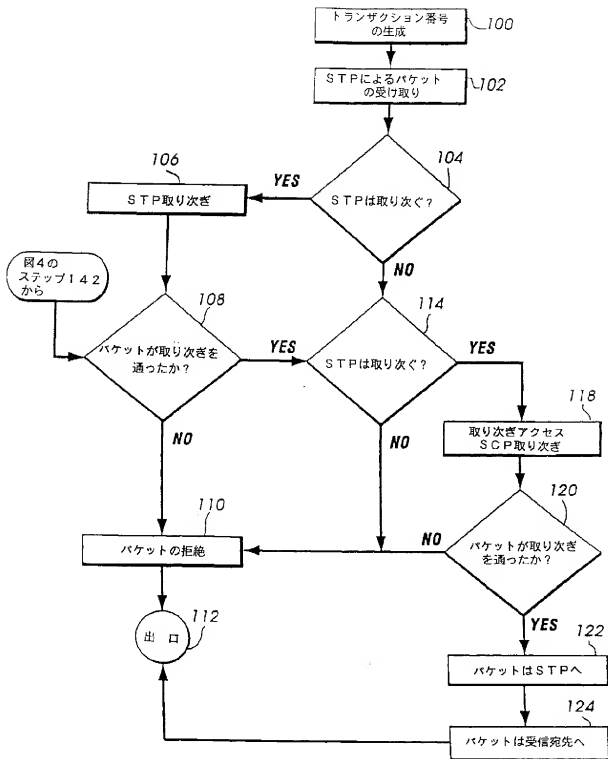
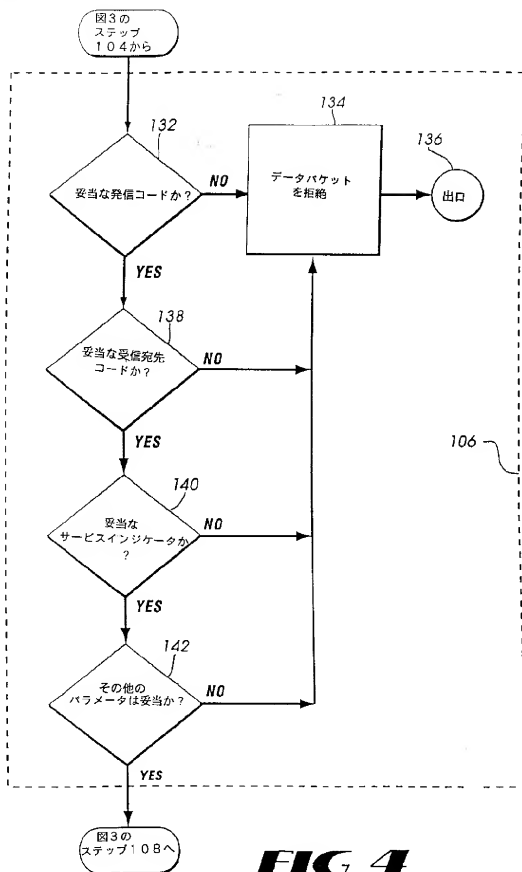
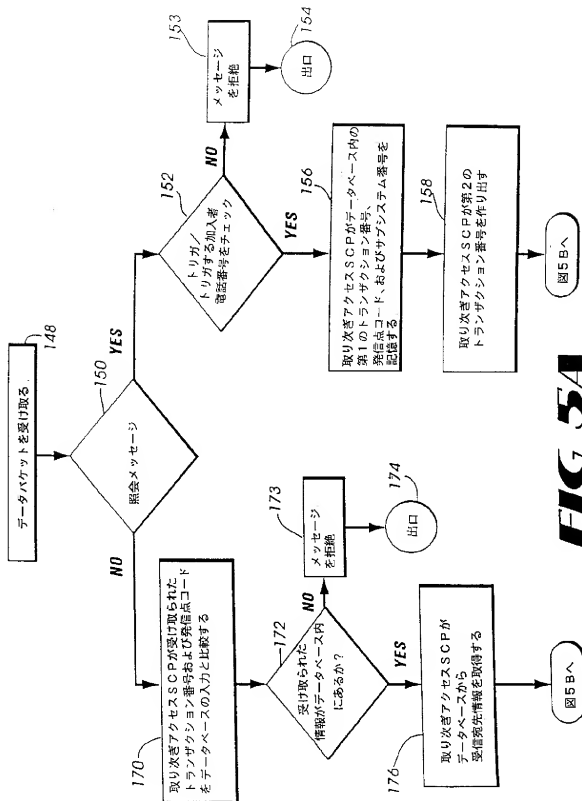
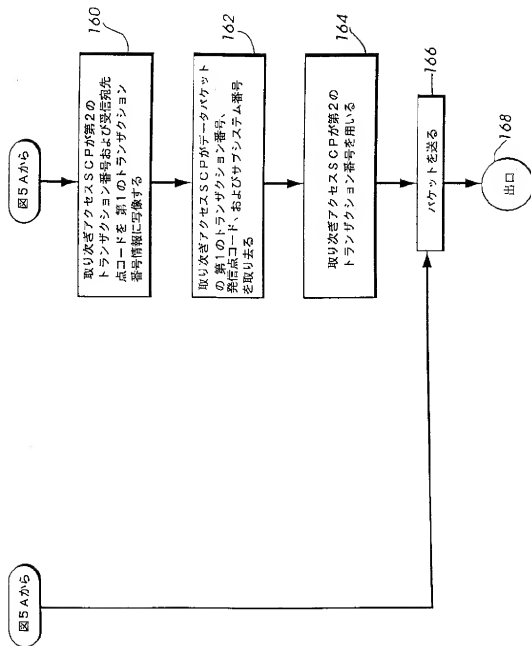


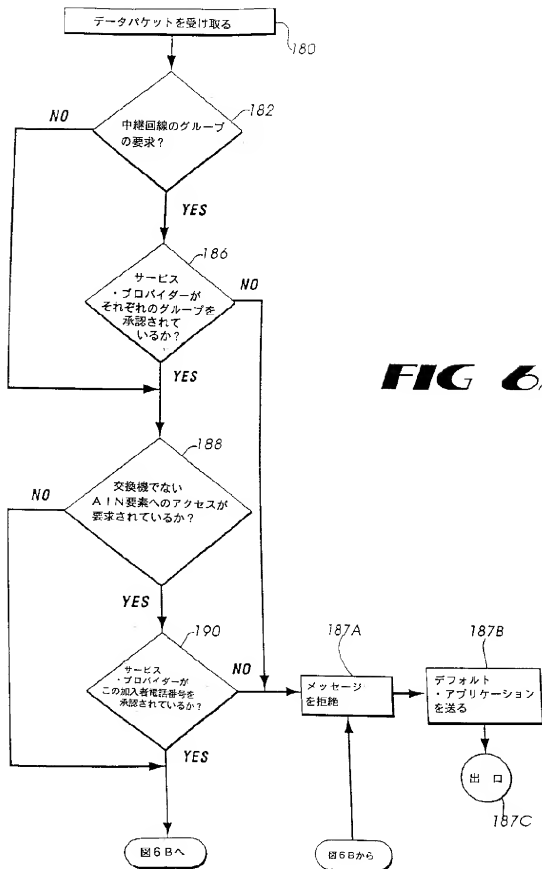
FIG 3

**FIG 4**



**FIG 5B**

【図 6】



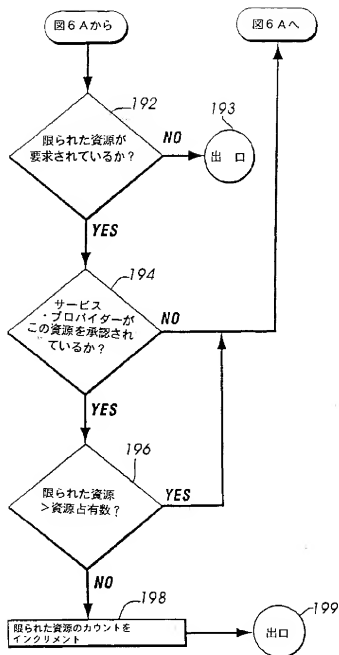
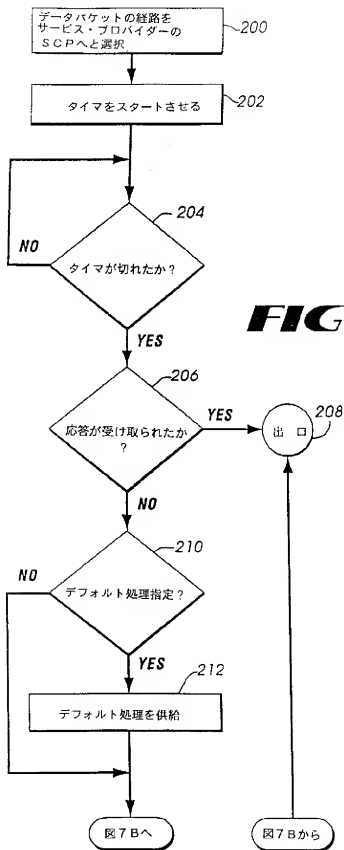


FIG 6B



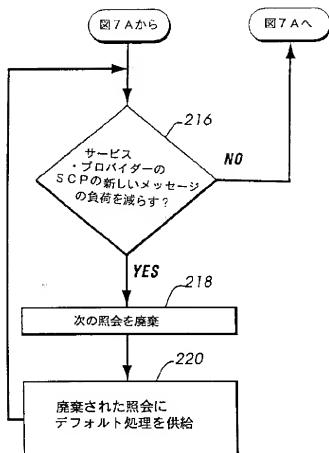


FIG 7B

【図 8】

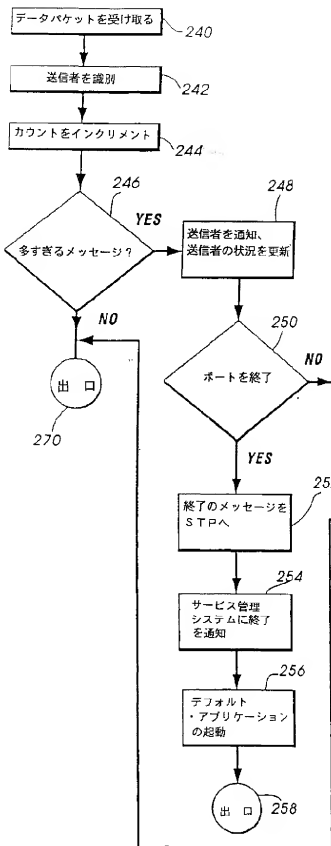


FIG 8A

図 8 B へ

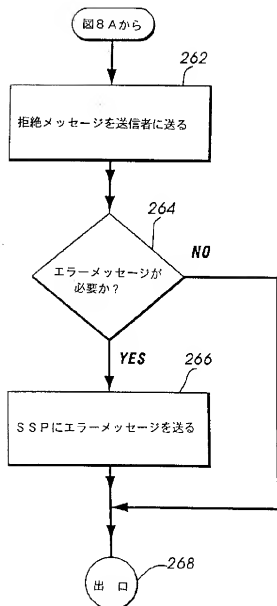


FIG 8B

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 95/07077

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q3/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04Q H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indications, where appropriate, of the relevant passages	Relevant to claim No.
X	TELEPHONY, vol.226, no.18, 2 May 1994, US pages 68 - 72 THEUS ET AL. 'Open access to the intelligent network: The road to more flexible and responsive services' see the whole document ---	1, 11, 14
X	IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, vol.1, 14 February 1994, KISSIMMEE US pages 140 - 152, XP000452403 CHEN 'Open AIN operations strategies' see page 145 - page 146 ---	1, 11
-/-		

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another claim(s) or raise special reason (see specification)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the invention but used to understand the principle or theory underlying the invention

- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "A" document member of the same patent family

Date of the actual completion of the international search

6 October 1995

Date of mailing of the international search report

6. 12. 95

Name and mailing address of the ISA

European Patent Office, P.O. 5113 Patentaan 2
NL - 2280 HV Rijswijk
Tel.: (+31-70) 340-2046, Tlx. 31 631 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

S J LAMBLEY

INTERNATIONAL SEARCH REPORT

national Application No
PCT/US 95/07077

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TELEPHONY, vol.226, no.22, 30 May 1994, US pages 24 - 25 JOHNSON 'Provisioning AIN services' see ---	1,8-11, 14-18
A	US,A,4 310 727 (LAWSER) 12 January 1982 see column 2, line 53 - column 3, line 56; figure 2 ---	1-4,7-9, 19-28
A	GLOBAL TELECOMMUNICATIONS CONFERENCE, vol.1, 15 November 1987, TOKYO JP pages 112 - 116 BOESE ET AL. 'The multimedia SCP' -----	

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos. _____
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos. _____
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos. _____
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE SHEET B

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos. _____.
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos. _____.

1-28, 35-37

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

LACK OF UNITY OF INVENTION

1. Claims: 1-28,35-37
2. Claims: 29,30
3. Claims: 31-34
4. Claims: 38,39
5. Claims: 40-43

The common or corresponding technical feature of independent claims 1,19,25,29,30,31,32,38,40 and 42 is an intelligent switched telephone network including a mediated access service control point, or a mediation method used in such a network.

The search revealed documents 'Open access to the intelligent network: The road to more flexible and responsive services' by Theus et al., and 'Open AIN operations strategies' by Chen, each of which are considered to represent the closest prior art and disclose a network with this technical feature (see p.72, left column, lines 36 to 59; and p.145 respectively).

There are five groups of technical features claimed, which do not contain either the same or a corresponding technical feature, as they relate to different objectively determined problems and their different solutions.

These are -

- A. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 1,19 and 25 (and their dependent claims) with respect to this prior art are -
replacing certain data within an IN message with a second set of data, storing the original data, and then routing the message accordingly if data in a received message corresponds to stored data, solving the objectively determined problem of mediation of routing messages generated as a result of connection to one of a variety of service providers.
- B. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 29 and 30 with respect to this prior art are -
checking a table of trunk route groups and a table of authorised directory numbers for correspondence to a parameter in an IN message, solving the objectively determined problem of ensuring that received parameter values correspond to values in the original data packet.

./.

- C. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 31 and 32 (and its dependent claims) with respect to this prior art are - using a count of the occupancy of resources, and rejecting messages or introducing gapping as appropriate to prevent overload, solving the objectively determined problem of use of limited network resources offered by a service provider.
- D. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claim 38 (and its dependent claim) with respect to this prior art are - sending a test message to an out-of-service SCP and re-classifying the SCP as in-service if it responds properly, solving the objectively determined problem of monitoring the status of an SCP that has been determined as out-of-service.
- E. The special technical feature, as defined in Rule 13.2 PCT, second sentence, included in claims 40 and 42 (and their dependent claims) with respect to this prior art is - introducing an auditable parameter into the IN message, solving the objectively determined problem of auditing IN messages, for security or other purposes.

Consequently, the claims do not fulfill the requirement of unity (Rule 13 PCT).

INTERNATIONAL SEARCH REPORT

Information on patent family members.

International Application No.

PCT/US 95/07077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4310727	12-01-82	NONE	

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, MW, SD, SZ, UG), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN

【要約の続き】

する情報に対応する情報をデータパケットから除去する。取り次ぎアクセスSCPは、この除去された情報を記憶し、代用情報を生成し、除去された情報をそのデータベース内の代用情報と相関させ、データパケット内の除去された情報を代用情報と取り替える。代用情報は、データパケットの受領者にネットワークの動作に関する情報を一切供給しない。応答データパケットを受け取ると、取り次ぎアクセスSCPは、応答データパケットを、代用情報を含んでいるか検査する。応答データパケットがこの代用情報を含んでいない場合には、データパケットは拒絶される。応答データパケットが代用情報を含んでおり、その他の点で妥当な場合には、取り次ぎアクセスSCPは、代用情報を除去された情報と関連させ、除去された情報を用いてさらにデータパケットの経路を選択する。

【公報種別】特許法第17条第1項及び特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成12年3月14日（2000.3.14）

【公表番号】特表平10-501396

【公表日】平成10年2月3日（1998.2.3）

【年通号数】

【出願番号】特願平8-502274

【国際特許分類第7版】

H04M 3/00

3/42

【F1】

H04M 3/00 A

3/42 A

手続補正書

平成11年10月4日

特許庁長官様

1. 事件の表示 平成9年特許第502274号

2. 補正の事由

明細書の誤脱

図面又は図説

特許代理人

ベネッセ コーポレーション

3. 代理人

氏名

〒105 東京都港区赤坂1丁目3番3号

ビル101室（3階）

電話 東京（33464）3075（代）

手続上（3346）二行 特許

氏名

4. 補正の請求

請求の範囲

5. 補正の範囲

請求の範囲を別紙のとおり補正する。

特許請求の範囲

1. サービス・プロバイダーのサービス制御点（47）およびインテリジェント交換電話ネットワーク事業者間のデータパケットメッセージの転送されない送信を防止する方法であって、

前記ネットワークは、少なくとも1つの信号中継点（20'）を含む複数のインテリジェント交換ネットワーク要素、および少なくとも1つの送り先サービス制御点（26'）の間での複数のデジタルデータ通信チャネルを含み、顧客の記録を含む少なくとも1つのデータベース（45）を含み、前記送り先サービス制御点（26'）が前記信号中継点（20'）に接続されるものにおいて、

前記方法が、

前記信号中継点（20'）内で第1のトランザクション番号を有するメッセージを受け取る手段と、

前記メッセージを前記信号中継点（20'）から前記送り先サービス制御点（26'）へ送附する手段と、

前記送り先サービス制御点（26'）内の前記メッセージを送信する手段であって、

前記データベース（45）内に前記メッセージの第1のトランザクション識別子を記憶することと、

前記メッセージの第2のトランザクション番号を生成

成すること。

前記第2のトランザクション番号を前記データベース(45)内の前記第1のトランザクション識別子と関連付けること。

前記メッセージから前記第1のトランザクション番号を削除すること。

前記メッセージに前記第2のトランザクション番号を付加すること。
なら成る手順と
を含むことを特徴とする方法。

2. 前記トランザクション識別子を記憶する前に、メッセージ情報として前記メッセージを読み取ること。
前記メッセージ情報を前記データベース(45)内の少なくとも1つの顧客の前帳に照合するかと比較することと、
前記メッセージ情報が前記顧客の記録と対応しない場合には前記メッセージを拒否することと
をさらに含むことを特徴とする請求項1に記載の方法。

3. 前記トランザクション識別子が、前記第1のトランザクション番号、前記メッセージの発信コード、および前記メッセージのサブシステム番号を有し、
前記トランザクション識別子を記憶する手順が、前記第1のトランザクション番号、前記発信コード、および

前記サブシステム番号を記憶する手順を含むことを特徴とする請求項1に記載の方法。

4. 前記メッセージが、前記第1のトランザクション番号、前記発信コードおよび前記サブシステム番号を有し、
前記第1のトランザクション番号を削除する手順が前記第1のトランザクション番号、前記発信コード、および前記サブシステム番号を前記メッセージから削除する手順を含むことを特徴とする請求項3に記載の方法。

5. 前記データベース(45)内で活動状態にある第2のトランザクション番号のリストに前記第2のトランザクション番号を記憶する手順をさらに含むことを特徴とする請求項2に記載の方法。

6. 前記第2のトランザクション番号は割り当てられていない疑似番号であり、前記第2のトランザクション番号を生成する前記手順が前記割り当てられていない疑似番号を前記第2のトランザクション番号として生成する手順を含むことを特徴とする請求項2に記載の方法。

7. 前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ手順が、
前記メッセージが前記メッセージかどうかを決定する

手順と、

前記メッセージが前記メッセージである場合には、前記前記メッセージのトランザクション番号を前記データベース(45)に記憶されている前記活動状態のトランザクション番号のリストに対応するか比較する手順と、
前記トランザクション番号が前記活動状態のトランザクション番号のリスト内の登録内容と対応しない場合には、前記メッセージを拒否する手順と
を含むことを特徴とする請求項1に記載の方法。

8. 前記トランザクション番号が活動状態のトランザクション番号の前記リストの登録内容に対応する場合には、前記登録内容から登録内容情報を取得する手順と、
前記登録内容情報に基づいて前記メッセージの機能を決定する手順と、
をさらに含むことを特徴とする請求項1に記載の方法。

9. 前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ手順が、
前記メッセージが前記メッセージに該当して前記サービス、プロバイダーのサービス制御点(47)から受け取る前記メッセージがあるかどうかを決定する手順と、
前記メッセージが前記サービス制御点の場合には前記前記メッセージが発信コードを含むかどうかを決定する手順と、
をさらに含むことを特徴とする請求項1に記載の方法。

前記前記メッセージが前記発信コードを含む場合には、前記発信コードが前記前記メッセージに関連した発信発信コードに照合するかと比較する手順と、
前記発信コードが前記発信コードに対応しない場合には、前記メッセージを拒否する手順と、
をさらに含むことを特徴とする請求項1に記載の方法。

10. 前記取り次ぎアクセスサービス制御点(26)の前記メッセージを取り次ぐ前記手順のあとに、前記メッセージが前記取り次ぎアクセスサービス制御点(26)内の取り次ぎを通過したかどうかを決定する手順と、
前記メッセージが前記取り次ぎアクセスサービス制御点(26)内の取り次ぎを通過した場合には、前記サービス、プロバイダーのサービス制御点(47)がサービス外であるかどうかを決定する手順と、
前記サービス、プロバイダーのサービス制御点(47)がサービス外の場合には、前記メッセージを拒否し、前記メッセージをデフォルト応答で提供する手順と、
をさらに含むことを特徴とする請求項1に記載の方法。

11. 前記メッセージが特定のサービス、プロバイダーのサービスの要求を有し、
前記サービス、プロバイダーのサービス制御点(47)がサービス外であるかどうかを決定する前記手順と、
をさらに含むことを特徴とする請求項1に記載の方法。

前記特定のリーバース・フロバイダーのサービスがサービス外であるかどうかを決定する手順と、

前記特定のリーバース・フロバイダーのサービスがサービス外である場合には、前記メッセージを拒否し、前記メッセージを前記デフォルト宛で提供する手順とを含むことを特徴とする請求項1に記載の方法。

1.2. 前記符号中継点(20')内で前記メッセージを受け取る前記手順のあとに、前記メッセージを前記フロバイダーのサービス中継点(47')から発信するかどうかに決定する手順と、

前記メッセージを前記フロバイダーのサービス中継点(47')から発信する場合には、前記符号中継点(20')内の前記メッセージを最終に取り次ぐ手順とをさらに含むことを特徴とする請求項1に記載の方法。

1.3. 前記メッセージが発信元コードを備え、

前記符号中継点(20')が前記符号中継点(20')へのメッセージの各承認されたフロバイダーのポート識別子を有し、

前記符号中継点(20')で前記メッセージを最終に取り次ぐ手順が、

前記発信元コードを少なくとも1つのポート識別子に対応するか比較することと、

前記発信元コードが前記ポート識別子のいずれにも

含むことを特徴とする請求項1.4に記載の方法。

1.6. 前記メッセージがサービスインジケータを有し、前記符号中継点(20')は、前記符号中継点(20')へのメッセージのそれぞれの承認されたフロバイダーの承認されたサービスを決定する少なくとも1つのサービスインジケータを有し、

前記符号中継点(20')内の前記メッセージを最終に取り次ぐ手順が、

前記サービスインジケータが少なくとも1つの承認されたサービスインジケータに対応するか比較すること、および

前記サービスインジケータが前記承認されたサービスインジケータのいずれにも対応しない場合には、前記メッセージを拒否することを含むことを特徴とする請求項1.2に記載の方法。

1.7. 複数のネットワーク要素間の複数のデジタル直接チャネルを備えるインテリジェント交換電話ネットワークにおいてパケットメッセージのトラヒックを取り次ぐ方法において、前記方法が、

新しいトラランザクション性能アプリケーション部メッセージを急送する前記複数のネットワーク要素の第1のものに、再行記録しいトラランザクション性能アプリケーション部メッセージの第1のトラランザクション番号を発

行しない場合には、前記メッセージを拒否することを含むことを特徴とする請求項1.2に記載の方法。

1.4. 前記メッセージが受信元コードを含む、

前記符号中継点(20')が、前記符号中継点(20')へのメッセージの各承認されたフロバイダーのメッセージ承認された発信元を決定する少なくとも1つの承認されたアドレスを有し、

前記符号中継点(20')内で前記メッセージを最終に取り次ぐ前記手順が、

前記受信元コードが少なくとも1つの承認されたアドレスに対応するかを比較する手順と、

前記受信元コードが前記承認されたアドレスのいずれにも対応しない場合には前記メッセージを拒否する手順とを含む

ことを特徴とする請求項1.2に記載の方法。

1.5. 前記承認されたアドレスの1つが前記取り次ぎアプリケーション部要素のアドレスを含む、

前記比較する手順が、前記発信元コードが前記取り次ぎアプリケーション部要素(26')の前記アドレスに対応するか比較することを含む、

前記拒否する手順が、前記受信元コードが前記取り次ぎアプリケーション部要素(26')の前記アドレスに対応しない場合には前記メッセージを拒否することと

をさせる手順と、

前記第1のネットワーク要素が前記複数のネットワーク要素のうち第2のものに前記トラランザクション性能アプリケーション部メッセージを送信する前に、前記第1のネットワーク要素に、前記第1トラランザクション番号を前記トラランザクション性能アプリケーション部メッセージに含ませる手順と、

前記第2のネットワーク要素に、前記トラランザクション性能アプリケーション部メッセージに関連した単一のトラランザクション識別子を生成させる手順と、

前記第2のネットワーク要素に、前記トラランザクション性能アプリケーション部メッセージの第2のトラランザクション番号を発生させる手順と、

前記第2のネットワーク要素に、前記トラランザクション性能アプリケーション部メッセージから前記第1のトラランザクション番号を削除させる手順と、

前記ネットワーク要素が前記トラランザクション性能アプリケーション部メッセージを別の受信宛先に送信する前に、前記第2のネットワーク要素に、前記トラランザクション性能アプリケーション部メッセージ内に前記第2のトラランザクション番号を含ませる手順と、

前記トラランザクション性能アプリケーション部メッセージと関連する特定のトラランザクションに影響を与えるが内部には前記第2のトラランザクション番号を含まない他のトラランザクション性能アプリケーション部メッセ

メソッドを前記ネットワーク要素にその後追加させる手順と、

を含むことを特徴とする方法。

18. 前記第1のネットワーク要素に、トランザクション識別子のテーブル内に前記第1のトランザクション番号を格納させる手順を含むことを特徴とする請求項17に記載の方法。

19. 前記第2のネットワーク要素に、前記第1のトランザクション識別子をトランザクション識別子テーブル内に記憶させることと、

第2のネットワーク要素に、前記第1のトランザクション識別子に関連した前記トランザクション識別子テーブル内に前記第2のトランザクション番号を記憶させることと、
を含むことを特徴とする請求項17に記載の方法。

20. 前記第1のネットワーク要素に前記第1のトランザクション番号を含む前記手順が、

前記第1のネットワーク要素に、前記第1のトランザクション番号およびメッセージ識別子と前記トランザクション情報アプリケーション部メッセージ内に含まれること
を含んで構成されることを特徴とする請求項17に記載

第1のトランザクション番号を含むメッセージを受信するネットワーク要素に、前記メッセージに関連した第1のトランザクション識別子を生成させることと、

前記ネットワーク要素に、前記メッセージの第2のトランザクション番号を付加させることと、
前記ネットワーク要素に、前記第1のトランザクション識別子に関連した第2のトランザクション番号を記憶させることと、

前記ネットワーク要素に、前記メッセージから前記第1のトランザクション番号を削除させることと、
前記ネットワーク要素に前記メッセージに前記第2のトランザクション番号を付加させることと、

前記サービス・プロバイダーのサービス側面(47)および前記ネットワーク要素に、その後、前記メッセージに関連した特定のトランザクションに影響を与える他のメッセージ内に前記第2のトランザクション番号を含ませ、前記第2のトランザクション番号を含まない前記他のメッセージを格納させることと

を含むことを特徴とする方法。

前記サービス・プロバイダーのサービス側面(47)および前記ネットワーク要素に、その後、前記メッセージに関連した特定のトランザクションに影響を与える他のメッセージ内に前記第2のトランザクション番号を含ませ、前記第2のトランザクション番号を含まない前記他のメッセージを格納させることと
を含むことを特徴とする方法。

24. 前記メッセージが格納先コードを含む、前記ネットワーク要素が前記ネットワークへのメッセージの各承認されたプロバイダーのポート識別子を備え、
前記方法が、
前記ネットワーク要素に、前記受信先コードをポ

の方法、

21. 前記トランザクション情報アプリケーション部メッセージが、受信先コード、およびサブシステム番号を含む、
前記第2のネットワーク要素に前記第1のトランザクション識別子を生成させる手順が、
前記第2のネットワーク要素に、前記第1のトランザクション番号と前記受信先コードおよび前記サブシステム番号とを格納することにより前記第2のトランザクション識別子を生成させること
を特徴とする請求項17に記載の方法、

22. 前記第2のネットワーク要素に前記第1のトランザクション番号を削除させる手順が、前記第2のネットワーク要素に、前記トランザクション情報アプリケーション部メッセージから前記第1のトランザクション番号、前記受信先コード、および前記サブシステム番号を削除させることを特徴とする請求項21に記載の方法、

23. サービス・プロバイダーのサービス側面(47)および前記ネットワーク要素間の生成のデジタルデータ通信を含むインテリジェント交換ネットワークの間のパケットメッセージのトラフィックを取り扱う方法において、前記方法が、

23. サービス・プロバイダーのサービス側面(47)および前記ネットワーク要素間の生成のデジタルデータ通信を含むインテリジェント交換ネットワークの間のパケットメッセージのトラフィックを取り扱う方法において、前記方法が、

識別子に対して比較すること、および
前記ネットワーク要素に、前記受信先コードが前記ポート識別子のいずれにも対応しない場合には前記メッセージを拒否すること
をさらに含むことを特徴とする請求項23に記載の方法。

24. 前記メッセージが受信先コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認された受信先先を指定する少なくとも1つの承認されたアドレスを有し、
前記ネットワーク要素に、前記受信先先コードが少なくとも1つの承認されたアドレスに対応するか比較させる手順と、
前記承認先先コードが前記承認されたアドレスのいずれれにも対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

25. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

26. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

27. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

28. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

29. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

30. 前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認されたサービス側面を指定する少なくとも1つのサービスインジケータを有し、
前記ネットワーク要素に、前記サービスインジケータが前記承認されたサービス側面に対応するか比較させる手順と、
前記サービスインジケータが前記承認されたサービス側面に対応しない場合には、前記ネットワーク要素に前記メッセージを格納させる手順と、
を含むことを特徴とする請求項23に記載の方法、

前記ネットワーク要素に、前記サービスインジケータが少なくとも1つの登録されたサービスインジケータに対応するか比較させる手順と、

前記サービスインジケータが前記承認されたサービスインジケータに対応しない場合には、前記ネットワーク要素に前記メッセージを拒否させる手順とを含むことを特徴とする請求項2に記載の方法。

31. サービス・プロバイダーのサービス制御点(47)および取り次ぎアクセスサービス制御点(26')を含むインテリジェント交換機ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法は、

前記取り次ぎアクセスサービス制御点(26')に、前記サービス・プロバイダーのサービス制御点(47)の指定の中継点のグループインデックスのグループを維持させる手順と、

前記取り次ぎアクセスサービス制御点(26')が前記指定の中継点の登録要求を含むメッセージを受け取ることに応じて、前記取り次ぎアクセスサービス制御点(26')に、前記指定の中継点のグループの熟達に対応する登録内容の前記テーブルをフェッチさせる手順と、

前記指定の中継点のグループの熟達を前記テーブル内の登録内容に対応しない場合には、前記取り次ぎア

クセスサービス制御点(26')に前記メッセージを拒否させる手順とを含むことを特徴とする方法。

32. サービス・プロバイダーのサービス制御点(47)、および取り次ぎアクセスサービス制御点(26')を含むインテリジェント交換機ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、

前記取り次ぎアクセスサービス制御点(26')に、前記サービス・プロバイダーのサービス制御点(47)のネットワーク要素の登録された加入者電話番号のテーブルを維持させる手順と、

前記取り次ぎアクセスサービス制御点(26')がネットワーク要素へのアクセスの要求を含むメッセージを受け取ることに応じて、前記取り次ぎアクセスサービス制御点(26')に、前記ネットワーク要素の加入者電話番号に対応する登録内容の前記テーブルをチェックさせる手順と、

前記加入者電話番号が前記テーブル内の登録内容に対応しない場合には、前記取り次ぎアクセスサービス制御点(26')に前記メッセージを拒否させる手順と、を含むことを特徴とする方法。

33. サービス・プロバイダーのサービス制御点(47)

および取り次ぎアクセスサービス制御点(26')を含むインテリジェント交換機ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法は

前記取り次ぎアクセスサービス制御点(26')に、前記サービス・プロバイダーのサービス制御点(47)の指定された直訳点の数を維持させる手順と、

前記取り次ぎアクセスサービス制御点(26')に、前記サービス・プロバイダーのサービス制御点(47)が占有している数値の現在のカウンタを維持させる手順と、

前記取り次ぎアクセスサービス制御点(26')がネットワーク要素の転送を含むメッセージを受け取ることに応じて、前記現在のカウンタが前記指定された直訳点の数と等しいかそれより大きい場合には、前記取り次ぎアクセスサービス制御点(26')に前記メッセージを拒否させる手順とを含むことを特徴とする方法。

34. サービス・プロバイダーのサービス制御点(47)および取り次ぎアクセスサービス制御点(26')を含むインテリジェント交換機ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法は、

前記取り次ぎアクセスサービス制御点(26')に、前記

サービス・プロバイダーのサービス制御点(47)が特定の時間内に収まないメッセージの現在のカウンタを維持させる手順と、

前記現在のカウンタが特定のカウンタと等しいかそれを上回った場合には、前記取り次ぎアクセスサービス制御点(26')に前記サービス・プロバイダーのサービス制御点(47)に提供されるメッセージの数を減少させる手順とを含むことを特徴とする方法。

35. 前記取り次ぎアクセスサービス制御点(26')にメッセージの数を減少させる前記手順が、前記取り次ぎアクセスサービス制御点(26')に、前記サービス・プロバイダーのサービス制御点(47)宛ての次のメッセージを拒否させる手順を含むことを特徴とする請求項30に記載の方法。

36. 前記ネットワークが前記サービス・プロバイダーのサービス制御点(47)をサービスする少なくとも1つのサービス交換機(15)を含む。

前記取り次ぎアクセスサービス制御点(26')にメッセージ数を減少させる前記手順が、前記取り次がれたアクセスサービス制御点(26')に自動発呼キッキングのメッセージを前記サービス交換機(15)に送る手順を含むことを特徴とする請求項30に記載の方法。

3.3. サービス外のサービス・プロバイダーのサービス解凍点を試験する手順と、

前記サービス外のサービス・プロバイダーのサービス解凍点が前記試験に適切に反応した場合には、前記サービス外のサービス・プロバイダーのサービス解凍点をサービス中のサービス・プロバイダーのサービス解凍点として再分類する手順と

をさらに含むことを特徴とする請求項 1.0 に記載の方法。

3.4. 前記サービス外のサービス解凍点を試験する前記手順が、前記サービス外のサービス・プロバイダーのサービス解凍点に試験メッセージを送る手順を含むことを特徴とする請求項 3.3 に記載の方法。

3.5. 前記サービス外のサービス解凍点を試験する前記手順が、前記サービス外のサービス・プロバイダーのサービス解凍点に試験メッセージを宛先固有なアドレスで送る手順を含むことを特徴とする請求項 3.4 に記載の方法。

3.6. サービス外のサービス・プロバイダーのサービス解凍点および取り次ぎアクセスサービス点（2.6'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理

3.9. 前記監査可能な事象がメッセージを含む。前記監査可能な事象がメッセージの日付、時刻、トリガのタイプ、トリガする宛先番号、および前記メッセージのコピーから生成され、

前記監査可能な事象の監査記録を生成する手順が、前記メッセージの宛先日付、時刻時刻、前記トリガのタイプ、トリガする前記宛先番号、および前記メッセージの宛先コードを含む前記監査記録を生成することから成ることを特徴とする請求項 3.8 に記載の方法。

4.0. サービス・プロバイダーのサービス解凍点（4.7'）およびインテリジェント交換電話ネットワークの複数のネットワーク要素の間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法が、

前記ネットワーク要素の 1 つでセキュリティ監査要求パラメータを含むメッセージを受信することと、

前記セキュリティ監査要求パラメータを受信することに基づいて、前記ネットワーク要素の前記 1 つに前記メッセージのセキュリティパラメータを生成させることを含むことを特徴とする方法。

4.1. 前記ネットワーク要素に、その後、前記メッセージに関連する特定のトラッキングアクションに影響を与える他

する方法において、前記方法が、

前記サービス外のサービス・プロバイダーのサービス解凍点（4.7'）に試験メッセージを送ることと、

前記サービス外のサービス・プロバイダーのサービス解凍点が適切に前記試験メッセージで応答した場合に、前記サービス外のサービス・プロバイダーのサービス解凍点をサービス中のサービス・プロバイダーのサービス解凍点として再分類することと

を含むことを特徴とする方法。

3.7. 前記サービス外のサービス解凍点に試験メッセージを送る手順が、前記サービス外のサービス・プロバイダーのサービス解凍点に定期的に試験メッセージを送ることを特徴とする請求項 3.6 に記載の方法。

3.8. サービス・プロバイダーのサービス解凍点（4.7'）および取り次ぎアクセスサービス点（2.6'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法が、

前記取り次ぎアクセスサービス点（2.6'）に、データパケットメッセージ内の前記取り次がれたトラヒックについての監査可能な事象を生成させる手順と、

前記監査可能な事象の監査記録を生成する手順とを含むことを特徴とする方法。

のメッセージとともに前記セキュリティパラメータを生成させる手順をさらに含むことを特徴とする請求項 4.0 に記載の方法。